APPLICATION FOR PATENT

INVENTOR: **BALAMANI S. VISHWANATH AND BRIAN D. MANTZ**

TITLE: **SECURE ECOMMERCE TRANSACTION AND USER/PRODUCT AUTHENTICATION MANAGEMENT SYSTEM**

SPECIFICATION

This application is a continuation-in-part application of United States Patent Application Serial No. 09/847,465, filed May 2, 2001, which relies upon U.S. Provisional Patent Application Serial No. 60/211,822 filed June 15, 2000.

Field of the Invention

The system relates to multiple facets of ecommerce, security, and processing between Sellers, Buyers, Financial Institutions, and Sources in addition to Sellers and Financial Institutions desiring additional transaction risk management, system user authentication and security or product authentication.

Background of the Invention

E-Payments

With the explosion of the Internet and meteoric rise in e-commerce, the need for better technologies and solutions for enabling secure online transactions has surfaced. According to TR's Online Census, compiled by Telecommunications Reports International (TRI), "more than 5 million US buyers joined the online world during the first quarter of 2000, an increase of 11% since the end of 1999, and a whopping 62% more than a year ago." (Source: CyberAtlas, 5 Million US Consumers Go Online in Q1). FIG. 1 shows the projected revenues for 1999-2003. In addition, an estimated 135.7 million users was forecasted to be on the Internet by the end of

1

2000 (Source: CyberAtlas, The World's Online Populations, May 1, 2000). Per Forrester Research, online sales are estimated to reach $143 billion by 2003, representing just 6% of the total retail market (Source: Forrester Research, 2000), with B2B sales reaching Trillions of dollars.

5   According to a key finding in a recent IDC report titled "Online Nation: A Survey of U.S. Web Buyers and Non-buyers", non-buyers actually represent a much larger percent of the US population than online buyers. Several reasons have been cited for why the majority of buyers hesitate to shop online, such as, lack of security and privacy.

Online security is a major barrier to expanding e-commerce. A new survey, conducted

10   by Washington DC-based SWR Worldwide, found that 64% of Internet users have reservations about online credit card transactions. Consequently, this concern severely impacts the purchasing behavior of online procurement. However, if personal information such as account numbers were not required, there would be a substantial increase in online buying. Nearly nine out of ten (87%) Internet users say they would be either "very likely" (52%) or "somewhat

15   likely" (35%) to use a credit card if they were not required to give out their credit card number to make purchases online (Source : PRNewswire, April 27, 2000). In a Business-to-Business commerce environment, Credit Cards are not the preferred payment method, due to the high value of an average transaction ($50,000 - $75,000 per transaction).

According to Meridien's findings, up to 15% of all Internet sales are potentially fraud-

20   related. They go on to predict that fraudulent transactions will amount to $9 billion in 2001 and increase to $15 billion in 2003. In recent months, several instances have been reported in the news highlighting the severity of online credit card fraud. Some examples of this are:

- Visa reported that 485,000 credit card numbers were stolen from a major e-teller in January 1999. The file was stored on a prominent government computer and the perpetrator was

25   traced to an Eastern European country (Source: E-Commerce Times Staff, Credit Card Fraud Crippling Online Merchants, March 20, 2000).

2

- Expedia.com, a spin-off of Microsoft and an online travel agency, will record $4-6M in third quarter losses to cover fraudulent credit card purchases made on its Web site (Source: E-Commerce Times Staff, Expedia Stung by Major Credit Card Fraud, March 2, 2000).

- CD Universe reported that a hacker stole 300,000 credit card numbers from its site

5   earlier this year (Source: E-Commerce Times Staff, Expedia Stung by Major Credit Card Fraud, March 2, 2000).

Credit-card fraud against online Sellers is on the rise. Since there is no face to face with a customer or signature with online purchases, Sellers are left without any recourse. While federal laws limit consumer liability to $50 or even $0, credit card companies force Sellers

10   to bear the entire loss. Additionally, in an effort to minimize their exposure, MasterCard will now fine Sellers $25K and up if charge-backs are 1% or higher of total sales transactions, or 2.5% or higher of total sales volume for more than 2 consecutive months. These penalties could force smaller e-commerce Sellers off the Web. Many online Sellers resent the inadequate support that they receive from the credit card companies. Currently, credit card companies only

15   verify that the credit card number is valid and then match the number against the customer's billing address. When a consumer indicates an instance of fraud, the disputed amount is removed from the Seller's account and credited back to the consumer. This charge-back comes with a standard fee of $15 per instance. Charge-backs represent substantial overhead to the Sellers because of the manual effort involved. Cyber-crime, in all forms, shows no signs of letting up.

20   Consequently, Sellers are being forced to utilize significant in-house resources to combat the problem or to buy expensive fraud-detection packages (Source: E-Commerce Times Staff, Credit Card Fraud Crippling Online Merchants, March 20, 2000).

In spite of the security issues, the predominant method of online payment today is still the credit card. However, many Buyers do not possess or qualify for a credit card.

25   According to the Online Finance Survey in the May 2000 issue of The Economist, cash continues to be the preferred method of payment for business-to-consumer transactions.

3

FIG. 2 shows the total United States consumer payments for 1998 from The Economist, May 2000. Despite consumer preference for cash over credit cards, a very limited number of online Sellers accept other forms of payment outside of credit cards. Consequently, Buyers are compelled to use credit cards for online purchases. In order for the world of e-commerce to be more widely accepted and accessible to the general consumer, other payment methods outside of credit cards will need to be adopted for online payment transactions. By restricting a Buyer's payment options to only credit cards, Sellers are limiting their revenue potential.

Banks have not been quick in responding to the opportunity to play the "Internet game" even though studies show that Buyers prefer checks or cash payments over credit cards. Since banks are viewed by their customers as a trustworthy agent and perceived to be financially strong and secure, they can utilize the Internet to expand their knowledge of customer behavior and purchasing patterns. In doing so, this provides them the power to increase their payment landscapes and develop profitable relationships with these most valued customers while keeping their competitors at bay. In order to stay on top, banks will need to look for new technological opportunities that provide an extensive role in the online arena. For instance, banks can exploit their core competency of payment processing for both businesses and Buyers, thus turning themselves into dominant online commercial intermediaries. Presently, a bank's role is limited to helping facilitate online payment transactions. By utilizing the technology that already exists, and taking advantage of the opportunities presented in the growing Internet space, banks could become a key player in this rapidly emerging marketplace.

It is vital that these Sellers be able to validate the online Buyers. Due to a decrease in fraudulent transactions and charge-backs, Sellers will notice a significant improvement to their bottom-line.

By offering Buyers payment options other than credit cards, the Seller's burden of credit card transaction fees will decrease. Transaction costs associated with alternative payment methods will be significantly lower than those for credit cards. Additionally, by offering these

4

alternative payment methods, Sellers will expand their potential consumer base to include those Buyers that either are non-credit cardholders or prefer not to use credit cards for online purchases.

Today, a large proportion of the population does not have access to online buying. However, online connections and PC ownership will soon expand to include low-income households, creating a new wave of e-commerce buyers.

In addition, there have been no truly successful attempts to provide a standardized interface between individual Seller Systems and a central system, such as the Smarte System^{TM}.

User Identity Management and Authentication

The economic perils currently encountered by online retailers are formidable. The Gartner Group reports, "The costs to e-businesses resulting from fraudulent transactions are expected to increase from an estimated $9 billion in 2001 to over $15 billion in 2003. Companies selling via the Internet must absorb the costs of disputes with users and of any fraudulent transactions they suffer. That's because online transactions lack a physical receipt that has been signed by the user and can later be verified. Online merchants eat the cost of all chargeback disputes."

Since 1997, the FTC (Federal Trade Commission) has maintained a Web-based database as a central part of its fraud-tracking program. "In 1997, there were fewer than 1,000 Internet fraud complaints. However, by 2000, that number had increased to over 25,000, roughly 26 percent of all fraud complaints logged." (www.FTC.com). Identity theft has earned the dubious distinction as the fastest growing crime in America. The relative anonymity and overwhelming reach afforded by the Internet combine to form the driving force behind the drastic increase in identity fraud. In order for online businesses to instill public confidence and to ultimately be successful, they must demonstrate that they can better address the issue surrounding the authentication of their users' true identities. Online travel industry leader Expedia.com illustrated this problem last year when it reported a US $4.1 million charge against revenues for fraudulent transactions. The use of simple usernames and passwords is not an adequate guarantor (legally or functionally) of user identification as this methodology only provides for one-factor authentication, which is

5

highly insecure. In the U.S., for example, Internet hackers reportedly stole 147,000 AOL passwords during November of 2000 (Austin-American Statesman). Passwords can be easily compromised through several methods including:

- Simple Guessing - users often choose simple, easy to remember passwords that can be
5 inferred.

- Theft - several types of software exist that perform network monitoring, keystroke monitoring, and password cracking functions which allow hackers to easily capture active passwords.

- Social Manipulation - people can often be manipulated into giving out their passwords,
10 for instance, to someone claiming to be a member of their company's technical support department.

Because the standard use of the credit card over the Internet only requires the credit card number (card not present transactions), a vast majority of Internet transactions are essentially based only on simple one-factor 'something the user knows' authentication.

15 "Credit card fraud is the biggest risk for the e-merchants. While all businesses accepting credit cards face this, the Internet merchant is even more exposed. Brick-and-mortar businesses can verify a signature to prove the authenticity of the payment, but there is no such protection yet for businesses on the Internet. Due to this increased risk, the credit card banks hold Internet merchants 100% liable for the losses and expenses incurred as a result of credit card fraud. The
20 defrauded merchants not only suffer because of the loss of product or services, but they are expected to pay a charge to defray the expenses the bank incurred from dealing with the fraud." – Gartner Group.

Moreover, businesses have to allot significant budgets towards maintaining network management departments that constantly have to tend to lost passwords, misused passwords, and
25 fraud on the Internet. In fact, the Gartner Group estimates that lost or forgotten passwords alone account for 20-50% of all corporate help desk calls.

From a consumer's perspective, the fear and apprehension surrounding the threat of identity theft results in a lower inclination to take advantage of all that the Internet has to offer. Half of all Internet users refuse to buy online because of their justified fears surrounding identity fraud and the Internet (epaynews.com). This prevailing consumer attitude has significantly curtailed e-business revenue growth in terms of both numbers of transactions as well as transaction dollar amounts. By instilling strong consumer confidence in e-business' ability to protect online identities, a strong user authentication solution converts window shoppers into real customers.

Passwords and simple one-factor authentication models do not positively identify a user, provide an audit trail of user activity, or provide user accountability. A powerful physical authentication mechanism that uniquely, conveniently, and cost effectively provides true user identification and non-repudiation while providing an optional platform for a single universal login/password to allow user access to multiple accounts will set a formidable precedent in the online arena.

Enterprise Application Access and Installation Management

As a significant number of enterprise software applications involve and generate highly sensitive intra-business information, there is an inherent need to restrict internal (to the enterprise) access to these types of applications. Currently, most enterprise software access is secured only by simple usernames and passwords. And as usernames and passwords are simply 'something the user knows', these bits of information only provide a highly insecure form of one-factor user authentication within an Intranet environment. The same tools and methods used to compromise passwords in an Internet environment are equally effective in an Intranet environment.

Alternative device-based enterprise user authentication solutions are extremely cost-prohibitive in terms of implementation and maintenance as well as device procurement. The clear need is for an application-driven device-based solution around which developers can construct a sound, affordable user authentication solutions appropriate to specific products and their environments.

A separate, but related issue to that of enterprise software access management is that of enterprise software installation management. Installation agreement enforcement is essentially relegated to the enterprise software purchaser on a 'good faith' basis. The larger and more

7

diverse an enterprise is generally correlates with higher rates of installation mismanagement. Although many instances of enterprise installation abuse are, indeed, intentional, a significant number result simply from unintentional oversights. Therefore, an effective method to manage application use with respect to defined license agreements would not only benefit the software

5   manufacturer, but the enterprise customer wishing to comply with those license agreements.

Software Piracy Management

The Software and Information Industry Association (SIIA) disclosed in its 2000 Report on Global Software Piracy that revenues lost by manufacturers of business applications software alone topped $11 Billion in the previous year. This report specifically concentrated on only

10   piracy of business application software and excluded piracy estimations regarding educational and entertainment software products. In a related report, the Business Software Alliance stated that the sum total of lost revenues to software manufacturers (of all types) due to piracy in the US alone was estimated to be $10.07 Billion for the same year.

One particular market segment, the entertainment software industry, clearly illustrates the

15   formidable economic hardships caused by piracy. The IDSA (Interactive Digital Software Association) states in a 2001 press release, "...our industry's piracy problems remain deeply entrenched and pervasive in far too many markets." The same press release cites from an IIPA (International Intellectual Properties Association) report, "...entertainment software industry losses in the 50 countries studied will once again exceed $3 billion," and continues, "... this $3

20   billion figure does not even include losses attributable to Internet piracy, nor losses in other major markets such as the U.S., Canada, Mexico, and much of Western Europe."

"The cost of worldwide piracy to the industry each year is staggering," states the IDSA in its 2000-2001 State of the Industry Report. In the same report, the IDSA reports total sales for the entertainment software industry for 2000 were just a shade over $6 billion. Relating the

25   industry piracy data to the industry sales figures indicates that the costs to the industry due to piracy approach that of its overall revenue generation. *For nearly every one dollar of legitimately sold entertainment software, another dollar's worth is pirated.*

8

According to the SIIA – "The numerous ways in which software piracy occurs, the ease of duplication and the high quality of pirated software present a significant problem for the software industry. A program that reflects unprecedented technology, years of effort and millions of development dollars can be duplicated or illegally distributed in minutes with the touch of a button. Any PC user can duplicate a product priced from $20 to $20,000 for no more than the cost of a blank CD or at no cost, and that user can make one, a dozen or a thousand functional copies."

Beyond the obvious negatives, software piracy does perform an invaluable service to most, if not all, companies within the industry. A software application's user base cannot be measured only by units and licenses sold as, in many cases, the number of illegitimate users approach or even outnumber legitimate users. The value of a broad and expanding application user base (whether legitimate or illegitimate purchasers) lies in its ability to generate new, legitimate sales.

A study published in the Journal of Marketing argues that more than 80% of legitimate software sales, within particular market segments, result from or are positively influenced by products that have been pirated.

Pirated software clearly holds significant value to its original manufacturer/publisher:

o Piracy expands company, brand, and specific product user bases.

o Piracy acts as a strong marketing vehicle, significantly extending the exposure of the company, brand, and product.

o Piracy can serve to provide 'trial' versions to potential and future legitimate purchasers.

Piracy is a global multi-billion dollar issue for software manufacturers of all types. As pirated products directly and indirectly lead to as much as 80% of legitimate sales in particular market segments, the desire on the part of the industry is to manage the issue to its economic advantage. Altogether or virtually eliminating the issue would only serve to eliminate extended product user bases and, hence, a substantial source of revenue. Within the industry, though,

9

needed piracy management features are highly variable based on market segments, competitive landscapes, and prevailing marketing strategies. The clear need is for an effective, affordable, and flexible solution that maximizes, on a company specific level, the formidable economic opportunities afforded through piracy management.

5

Summary of the Invention

The Smarte System™ is a software solution that provides new and unique solutions to the problems previously described. It does this through innovative and new forms of payment mechanisms, as well as providing levels of security unmatched in the industry. In addition to the payment mechanisms, a new and unique method of interface to existing seller systems, known as the Smarte VII™ Platform has been invented. Also, components of the Smarte System™ provide for strong user identity as well as software piracy management. These items are listed as follows:

Interface between Seller and Central System (Smarte VII™).

The Smarte VII™ platform serves as a true interface to the Seller's existing systems. It is based on a series of platform-independent applications that are custom configured at Seller sites. The platform provides MoveMoney™ a dynamic link to the Seller's database system. The platform also provides validation of the Seller through the unique authentication mechanisms, private/public key pair rings and the digital signatures programmed through the application. The Smarte VII™ infrastructure also provides the common ground and base structure needed for current applications as well as future product offerings.

Additional systems developed as part of the Smarte System™ are incorporated into he Smarte VII™ platform, such as a unified shopping cart, which provides the same look and feel across different Seller sites. The platform can also track multiple buys across different Seller sites by the same Buyer and group buying of the same product from the same Seller through different Buyers. Multiple currencies are a part of the system allowing international shopping with security, ease and comfort. Buying patterns are tracked to allow the Seller to streamline the

10

advertisements during checkout. Banner advertisements at different Seller web locations are made dynamic to facilitate rapid and instantaneous checkout, rather than a static advertisement that is more a nuisance to the online Buyers.

The Smarte VII™ architecture also ensures security by linking the Buyers and Sellers to the MoveMoney™ system, thus keeping track of the multiple sessions that are opened and closed during the checkout process. The design further allows for automatic encoding of all data using special hashing routines, and encrypting of the same data for security against spoofing. The Smarte VII™ platform keeps tracks of inventory and allows for appropriate and automatic updates to the Seller's inventory system. The application also profiles a link to a true B2B (business-to-business) application that facilitates procurement management and supply-chain management.

Checkout Application

Smarte Checkout™ is an application that is programmed at the Sellers' sites as a part of the Smarte VII™ platform installation. Smarte Checkout™ allows the Buyer to purchase products at the Sellers' sites with ease and comfort while being assured of a secure transaction. It also provides the Buyer with multiple payment methods and payment flexibility to complete the transactions. The Smarte Checkout™ technology provides security and instills confidence in the Buyer by preventing the transfer of sensitive financial information to the Seller.

Smarte Checkout™, working within the Smarte VII™ platform, tracks the entered electronic access information, and retrieves the appropriate profile information. The application waits for the double authentication from the Buyer and validates the information prior to displaying the profile information. Any changes to the default shipping address, payment type, payment options and shipping method is automatically updated and adjusted for price through the application. When the Buyer authorizes the transaction, Smarte Checkout™ confirms the transaction and forces the Smarte VII™ platform to update the Seller's database and close the connection to the MoveMoney™ server. Thereafter, the transaction database and the profile database are updated with the transaction information, and appropriate notifications are sent to

11

the Buyers and Sellers. Transactions are tracked for clearing, settlement and returns, and appropriate risk management techniques are applied to facilitate settlement with Buyers and Sellers.

Smarte Pay™ Application and Payment Types

Smarte Pay™ is a new and innovative MoveMoney™ payment technology that allows for multiple payment methods and payment flexibility at shopping sites. Smarte Pay™ serves to bring the Financial Institutions directly onto the forefront of the online payment processing.

Smarte Credit™ is a signature loan amount that the Financial Institutions offer to their Buyers in the event that funds are unavailable to honor their online transactions from their regular checking/savings/overdraft accounts. Smarte Credit™ helps in assuring that the online Sellers are guaranteed the funds to the extent that the Smarte Credit™ amount permits. With Smarte Pay™, Buyers have a choice, as well as the opportunity to split payments among various alternatives. Payment flexibility, by way of deferred payments, further enhances the Buyer's options during the checkout process. Buyers also have the flexibility to set appropriate limits within their Smarte Pay™ portfolio.

Smarte Cash™ (payments through the MoveMoney™ E-cash account), Smarte ATM™ (payments through the ATM network), Smart Cards (payments through stored value smart cards), E-cash (payments through third party electronic cash alternatives), private label cards (payments through private label cards such as Sears, JC Penny etc.), and credit cards (VISA, AmEx etc.) are also a part of the Smarte Pay™ system. The system also includes mechanisms for payments utilizing private third party loans as well.

Smarte Profile™

Smarte Profile is an online electronic profile for Financial Institutions, Buyers and Sellers. Sellers can have Sub-Sellers, Buyers can have Sub-Buyers and Financial Institutions can profile multiple branches within the system. The Smarte Profile™ maintains the appropriate personal profile information, as applied to the entity, as well as maintains a log of all transactions, messages, notifications, rewards, returns and updates.

12

Smarte Authentication[TM]

MoveMoney's two-factor authentication service combines "something the user knows", a username and password, with "something the user has", the Smarte Device[TM]. As passwords alone do not truly identify a user, Smarte Authentication[TM] greatly reduces the potential for and costs associated with identity fraud by establishing strong user accountability (true user non-repudiation) and by generating an audit trail of user activity. Smarte Authentication[TM] is an integrated security component of the Smarte Pay[TM] infrastructure which efficiently overcomes the failings of one-factor, password-only authentication systems. MoveMoney[TM] accomplishes strong two-factor digital authentication through the use of highly portable and easy to use Smarte Devices[TM]. Smarte Devices[TM] include software tokens that reside on handheld PDAs or WAP enabled cell phones, key chain tokens that generate a new authentication code every few seconds, and Smarte ID[TM]s – unique authentication devices developed and produced in-house by MoveMoney. Smarte Devices[TM] offer strong branding opportunities for partners and clients using Smarte Authentication[TM]. The Smarte ID[TM] itself is offered in two formats: as a wallet-sized CD or as a Smart Card. Using encrypted digital algorithms capable of being read by any type of CD drive or Smart Card Reader, the Smarte ID[TM] provides the convenient functionality of alternative two-factor authentication devices, but at a fraction of the cost. In addition to being an integral portion of the Smarte System[TM] itself, Smarte Authentication[TM] is structured/designed so that it can act as a stand-alone digital authentication service for third parties independent of the functions of the Smarte Pay[TM] infrastructure. Also, aside from user authentication, the Smarte ID[TM] (CD format) also provides product authentication to software manufacturers by preventing the unauthorized use of a product sold on the CD (anti-piracy solution).

Brief Description of the Drawings

FIG. 1 is a graph of ecommerce revenues;

FIG. 2 is a graph of total consumer payments;

FIG. 3 is a flowchart of primary system entity relationships;

13

FIG. 4 depicts basic system relationships of System Entities (non-user) to Financial Institutions;

FIG. 5 depicts basic system relationships of System Entities (non-user) to Sellers;

FIG. 6 depicts basic system relationships of System Entities (non-user) to Commercial

5 Buyers;

FIG. 7 depicts basic system relationships of System Entities (non-user) to Retail Buyers;

FIG. 8 depicts basic relationship between Authentication devices, External Sources, and

Lots;

FIG. 9 depicts basic system relationships of External Source's their system users and

10 devices;

FIG. 10 depicts basic system relationships regarding system Access Authorizations;

FIG. 11 depicts the basic system relationships regarding Product Authentication;

FIG. 12 depicts the placement of the Screen Identification Code (GUI) for Authentication

Screens;

15 FIG. 13 depicts Screen Layout for Main/Home Screens (All Users except Administrative);

FIG. 14 depicts Main Screen Layout for Financial Institution Users;

FIG. 15 depicts Main Screen Layout for Seller Users;

FIG. 16 depicts Main Screen Layout for Buyers (Both Commercial and Retail);

20 FIG. 17 depicts Main Screen Layout for MoveMoney™ Administration Users;

FIG. 18 depicts Financial Institution Management Screen Layout for Administration

Users;

FIG. 19 depicts Seller Management Screen Layout for Administration Users;

FIG. 20 depicts Independent Sales Org. Management Screen Layout for Administration

25 Users;

FIG. 21 depicts Buyer Management Screen Layout for Administration Users;

14

FIG. 22 depicts Transaction/Payment/Accounts Management Screen Layout for Admin. Users;

FIG. 23 depicts Authentication Management Screen Layout for Admin. Users;

FIG. 24 depicts Authentication Management Screen Layout for External Source Users;

FIG. 25 depicts Screen Layout for Authentication End Users;

FIG. 26 depicts the System Data Structure Layout and record relationships within the system;

FIG. 27 is a table containing the Table Names referenced in FIG. 26;

FIG. 28 is a visual representation of the Smarte CD™ Authentication Device;

FIG. 29 is a visual representation of the Smart Card Authentication Device;

FIG. 30 is a visual representation of the RSA™ SecurID™ Authentication Device;

FIG. 31 depicts the communication interaction between MoveMoney™ and other ecommerce entities;

FIG. 32 is a flow chart of the Smarte VII™ "Light" plug-in operational and communication flow;

FIG. 33 is a flow chart of the Smarte VII™ "Full" plug-in operational and communication flow;

FIG. 34 is a flow chart of the Smarte Authentication™ plug-in operational and communication flow for Type I Authentication use;

FIG. 35 is a flow chart of the Smarte Authentication™ plug-in operational and communication flow for Type II Authentication use;

FIG. 36 depicts the basic flow of Authentication Responses based on implementation;

FIG. 37 depicts the basic flow of Authentication Responses based on implementation in addition to those depicted in FIG 36;

FIG. 38 depicts Authentication Plug-in Information Passing Requirements

FIG. 39 is a flow chart of the Smarte Authentication™ system operational and communication flow for Product Authentication use;

15

FIG. 40 is a flow chart depicting the specific Authorization process for Smarte CD™ Devices;

FIG. 41 is a flow chart depicting the specific Authorization process for Smart Card Devices;

FIG. 42 is a flow chart depicting the specific Authorization process for 3rd party Devices;

FIG. 43 is a flowchart depicting the basic flow of the Smarte Authentication™ device/authorization process;

FIG. 44 depicts a typical Security Arrangement for hardware/software for 3rd party Authentication Processes, using MoveMoney's system as a portal only;

FIG. 45 depicts the basic "tier" structure of Transactions;

FIG. 46 is a flow chart depicting the "flow" of transactions from various initiation points/reasons;

FIG. 47 is a flow chart depicting the Determination of Fees/Commissions at the "Order" level;

FIG. 48 is a flow chart depicting the Determination of Transaction Generation Requirements;

FIG. 49 is a flow chart depicting Smarte Credit™ Initiation Process;

FIG. 50 is a flow chart depicting the Buyer Initiated Transfer Process;

FIG. 51 is a flow chart depicting the Overall Processing of Returned ACH Transactions;

FIG. 52 is a flow chart depicting the Process Requirements for ACH NSF type Returns;

FIG. 53 is a flow chart depicting the Process Requirements for ACH Returns for Bad or Incorrect RTN/Account;

FIG. 54 is a flow chart depicting the Process Requirements for ACH Closed Account type Returns;

FIG. 55 is a flow chart depicting the Process Requirements for ACH Info. Change type Returns;

16

FIG. 56 is a flow chart depicting the Process Requirements for ACH Transaction Buyer Authorization Denial and Transaction Authorization Revocation type Returns;

FIG. 57 is a flow chart depicting the Process Requirements for ACH R03 type Returns;

FIG. 58 is a flow chart depicting the Process Requirements for ACH Transaction Generation and Transmission;

FIG. 59 through 67 are examples of User Interface Requirements to Handle ACH Transaction R03 type Return Calculations.

FIG. 68 is a Table containing representative field data for Critical/Abnormal Activity Calculation;

FIGs. 69 through 71 are Tables containing representative field data for Smarte Credit ^{TM} Interest and Late Fee Calculations;

FIG. 72 is a flow chart detailing the logic and mathematics behind Late Fee Calculation;

FIG. 73 is a Table containing representative field data for Batch Payment Calculations (To Pay);

FIG. 74 is a Table containing representative field data for Batch Payment Calculations (Paid).

FIG. 75 depicts diagram displaying the Extended DLL data file structure;

FIG. 76 is a flow chart depicting the basic functional flow of the Standard DLL;

FIG. 77 is a flow chart depicting the basic functional flow of the Extended DLL;

FIG. 78 is a flow chart depicting the Validate Device function of the Extended DLL;

FIG. 79 is a flow chart depicting the Extended DLL Validate Device to Serial Number function;

FIG. 80 is a flow chart depicting the Extended DLL Add User ID function;

FIG. 81 is a flow chart depicting the Extended DLL Kill User ID function;

FIG. 82 is a flow chart depicting the Extended DLL Assign Device function;

FIG. 83 is a flow chart depicting the Extended DLL Unassign and Kill Device functions;

FIG. 84 is a flow chart depicting the Extended DLL Validate User function;

17

FIG. 85 is a flow chart depicting the Extended DLL Validate User ID Exists in System function;

FIG. 86 is a flow chart depicting the Extended DLL Return Device Info for User ID function;

FIG. 87 is a flow chart depicting the Extended DLL Identify User ID and Return Device Info functions;

FIG. 88 is a flow chart depicting the Extended DLL Import MoveMoney Device Info function;

FIG. 89 is a flow chart depicting the Extended DLL Initiate Datafile, Lock Datafile, Unlock Datafile, and Change Locked Datafile Password functions;

FIG. 90 is a flow chart depicting the function of the replication/duplication management software for non-serialized CD-ROMs only containing the media-based copy protection;

FIG. 91 is a flow chart depicting the function of the replication/duplication management software for serialized single set CD-ROMs;

FIG. 92 is a flow chart depicting the function of the replication/duplication management software for serialized sets of CD-ROMs;

FIG. 93 is an overview diagram depicting plug-in inter-system relationships;

FIG. 94 is a diagram depicting elements of MoveMoney's Identity Management Platform (Smarte User Authentication™);

FIG. 95 is a diagram depicting elements of MoveMoney's Software Access Management Platform (Enterprise Software Authentication™);

FIG. 96 is a diagram depicting elements of MoveMoney's e-Payment Management Platform (Smarte Pay™); and

FIG. 97 is a diagram depicting elements of MoveMoney's Piracy Management Platform (Smarte Product Authentication™).

18

Detailed Description of Preferred Embodiment

The following terms are used in this application.

Complete Entity Structuring

Complete Entity Interaction among Financial Institutions, Buyers, Sellers, Independent

5   Sales Organizations, Sub-Buyers, Traders, End-Users, Authentication Devices, Authorizations, Smarte Cash Accounts, Smarte Credit Accounts, Admin Accounts, and External Sources plus the ability to define and add any other Entity to the System.

Smarte Cash

A System payment mechanism and account type that allows the Buyer to allot a

10   dedicated amount from physical accounts (such as checking or savings) for online transactions.

Smarte ACH

A System payment mechanism that uses the ACH Network to allow users to use such physical accounts as checking and savings to make online purchases.

Smarte Credit

A credit account containing one or more individual user loan activations.

Admin Accounts

The structure for all internal administrative accounts is integrated within the System.

Authorization Protocols

The protocols that check user authorization for specific areas of the System are

20   integrated.

Access Protocols

The protocols that check user access to specific areas of the System are integrated.

Authentication Protocols

The protocols by which the System authenticates a user are integrated.

25   Reserves

The System allows for reserve amounts to be withheld from Sellers based upon specific transaction risk levels.

19

Holding Accounts

The structure for all MoveMoney holding accounts is integrated into the system.

Fees

Fee schedules and calculations are functional for all currently supported transaction types across all applicable entity types. Schedules can be user defined as both fixed, progressive, or a combination of both.

Commissions

Commission schedules and calculations are functional for all currently supported transaction types across all applicable entity types. Schedules can be user defined as both fixed, progressive, or a combination of both.

Smarte Interface

Sellers have two interface options for interaction with the System: a COM/XML plug-in or the more comprehensive Smarte VII Interface that includes a database management system.

Returns Processing

Charge-backs, non-sufficient funds (NSFs), and invalid account Returns are processed and compiled into a negative transaction history database.

Traceable Transactions

All transactions generated within the System are traceable to their root event.

Record Flags

Records with issues are flagged and maintained indicating current status (closed, pending, completed, etc.).

Smarte Credit Pay Down

Users have the proactive ability to pay down their Smarte Credit accounts within the System.

Federal Reserve Connections

All Federal Reserve connections (debit, credit, return) are integrated in the system.

Smarte Credit Interest Calculations

20

The interest calculation procedures are integrated to offer account management options such as individual activation grace periods and triggers.

Product Classes

Seller product offerings are broken into different Product Classes whereby specific products are grouped by applicable reserve amounts, fee/commission schedules, tax/shipping profiles, and risk levels.

Products

Sellers can upload images as well as provide pricing and product information within the system.

Logs and Reports

Activity logs and reporting features have been integrated within the System.

Split Pay

Buyers have the ability to split payments among multiple accounts across multiple vendors in a single order.

Smarte Catalog/iMall

A complete online Catalog/shopping mall within the System where Buyers can purchase multiple items from multiple Sellers in a single order.

Smarte Inventory

Smarte Inventory is an interface application available to Sellers participating in the Smarte Catalog/iMall. Smarte Inventory is an intelligent inventory search engine combined with MoveMoney's Smarte Ads feature.

Tax/Shipping Profiles and Calculations

Sellers define specific shipping locations, shipping methods, and tax structures for their product offerings. Based on these definitions, the System automatically performs applicable calculations.

User/Entity Profiles

All users and businesses within the System are defined by a basic set of information that comprises their Profile.

Notifications

The System contains an automated notification system defined by the user and triggered

5 by event type.

Identifiers

In addition to the basic set of information captured in the Profile, additional identifying information is captured by particular entities for particular users within the System. This feature enables a customization of Profile information.

10 Smarte ID

The System's dual authentication procedure is predicated on the use of devices (hard/soft) to verify the true identity of any user. The System has been developed to recognize these Smarte IDs during the authentication of a user.

User Signup Process

The System's user registration process allows for the choice of unique login names and password recovery questions.

Smarte ID Distribution Process

MoveMoney has defined multiple device distribution methodologies for use with Smarte Authentication as a stand-alone and in conjunction with the System.

20 Login Management

Across the entire System, every user login code must be unique. Upon the registration of a new user, the System performs a check against all existing logins to ensure the uniqueness of any new logins created.

Session and Security Protocols

25 Session Security Protocols have been designed and implemented. These include a user definable time-out feature based on user inactivity, a disabling of the browser 'Back' button, and

22

an inability of the user to have more than one session open at any one time. Also, the System uses session cookies as opposed to storage cookies.

Order Management

The System allows users to purchase from multiple Sellers and make payments from multiple account types all in a single order.

ACH, ATM, Cash, Credit Card Network Interfaces

The System is interfaced with and process transactions through all of the following networks: ACH, ATM, Cash, and Credit Card Networks.

Authentication Portal

MoveMoney's Authentication Portal (Smarte Authentication) is integrated into the Smarte System and is presented as a standalone offering as well. MoveMoney provides strong, two-factor user authentication through the use of such secure devices as CD-ROMS, ID Tokens, ID Business Cards (hard devices), and software installed on PCs, PDAs or wireless cell phones (soft devices).

ACH FED File Manager

ACH management application that accepts and manage multiple ACH file input formats.

Entity Tiers

The System entity structure includes Sub-FIs, Sub-Sellers, and Sub-Commercial Buyers. Also, Retail Sub-Buyers are able to tier below a Parent Retail Buyer.

Entity Crossover

The entity structure allows businesses to act as multiple entity types. A bank, for instance, could act as a Commercial Buyer and/or a Seller as well as operate as a Financial Institution within the System. This crossover also applies to entity users.

Rewards Program

The Rewards Program is integrated into the existing user structure to encourage user retention and increase user activity within the System.

Direct B2B Payments

23

Direct B2B payments application allows Businesses to transfer funds directly from/to one another.

B2B Exchange/Catalog Management

A complete online Buyer/Seller auction/reverse auction catalog management system.

Online Bill Pay/Presentment

Businesses present bills online and users pay those bills online.

Peer to Peer Transactions

Allows Buyers to transfer funds directly from/to one another.

Online Wire Transfers

Enables direct wire transfers between Financial Institutions.

Trigger Based Sales

Allows Sellers to create variable sales prices that are triggered based upon competitor sale prices. The System also allows Sellers to provide targeted advertising to its customers through Trigger Based Sales. Based on a customer's activity or purchasing habits within the store, the System generates product listings/ads of related items in which the customer may also be interested.

Portable Digital Signatures

A portable repository of digital signatures. Users are able to digitally sign documents from anywhere at any time by retrieving the portable repository through unique authentication.

International Funds Transfer

International Funds Transfer enables users to transfer funds internationally, in multiple denominations.

Wireless Transactions/Authentication

Smarte System access for transactions through wireless capable devices.

Point-of-Sale Transactions

Point-of-Sale transactions enable Brick-and-mortar establishments to offer direct Smarte System access to their customers.

24

Content Customization Server

This is a standalone application as well as an integrated feature within the System. It allows the user to define and create customized fields within web pages for capture and database inclusion of specifically desired information.

5   Electronic NSF Recovery

This application automates the recovery of funds generated by non-sufficient fund transactions.

Check to ACH Conversion

This application allows Sellers to generate ACH transactions directly from printed

10   checks.

Electronic Draft

This feature allows users to create electronic checking drafts.

Automatic Ad Generation

Automatically generates supplemental product listings to Buyers based on purchases just

15   made by the Buyer. For example, a Buyer purchases a camera and upon completion of the checkout process the Buyer is presented with the product information for film.

Expanded Notification System

The next level of notifications that allows System users to be electronically notified based on events occurring outside of the System.

20   Auction Site Hosting

The System can host B2C/C2C auction sites.

Banner Ads

Allows advertising through banner ads throughout the system.

Catalogs

25   Seller product inventories are consolidated and presented to Buyers in an online catalog format.

Certificates

25

As a repository for digital signatures, the System maintains a status of the Certificates.

Closing Functions

Mortgage and other financing processes are closed in an online format through the System.

5   Telecommunication Functions

The System incorporates voice communications through Internet capable devices such as laptops and computers.

Contract Signing

With digital signature and strong two-factor user authentication capabilities, contracts are

10   signed and delivered in an online format.

Currency Conversions

The System performs conversions of currency of multiple international denominations.

Online Coupons

Sellers can post and make available redeemable electronic coupons.

15   International Payments

Entities have the ability to transact business across international borders.

Site Hosting

Individual e-business sites can be hosted through the system individually or in conjunction with the Smarte Catalog/iMall.

20   Inventory Management

The System has the capability to manage all aspects of an e-business' product inventory in a web-based format.

Invoices

For B2B and applicable B2C environments, Invoices can be generated and distributed by

25   the System.

Complete Activity System Log

26

Complete activity histories for System Users and System Entities are generated within the system.

E-Mail Service

The System maintains a complete e-mail messaging system for all users.

Purchase Orders

Purchase Orders are generated and electronically sent through the System.

Send/Receive Payments

The System supports full person-to-person e-payment interaction.

SET Protocols

The SET e-commerce protocol are integrated to manage the risk involved during transmission of System information over the Internet.

Product Authentication

Software anti-piracy methodologies are incorporated within the scope of the System to allow software manufacturers to distribute software on CD-ROM media while significantly reducing exposure to piracy and illegal distribution.

Manufacturing Applications Interface

The System is designed to interface with all manufacturing management applications including, in particular, STEER™ from Elmaq Software™.

Online Voting

With its strong user authentication capability and risk management features, the System supports online voting processes.

The MoveMoney™ suite of Smarte™ offerings targets online businesses, B2B (Business to Business), B2C (business-to-consumer) and C2C (Consumer to Consumer) markets. The inter-system plug-in relationships of the system are depicted FIG. 93. The Financial Institutions and B2B Exchanges optionally help promote the MoveMoney™ technology to Sellers and Buyers for the many benefits that is derived by participating in this offering.

27

Sellers are provided a unique digital credential that validates them to the Buyers and the Buyers are provided a Smarte Device™ that uniquely identifies them to the Sellers. MoveMoney™ installs the application in the Seller sites and makes them "Smarte™" ready to attract online Buyers, providing them the unique benefits of security, convenience and alternate payment methods. Financial Institutions, Sellers and Buyers have their own Smarte Profiles™ that provides them with information on transactions, updates, logs, rewards and notifications.

The MoveMoney™ core technology is based on the Smarte VII™ platform that serves as an interface infrastructure linking the MoveMoney™ Smarte™ technology at Seller sites.

Smarte VII™ platform serves as a backbone to the entire MoveMoney™ Smarte™ product offerings. It is based on a series of platform-independent applications that are custom configured at Seller sites. The platform provides MoveMoney™ a dynamic link to the Seller's database system. The platform also provides for dynamic validation of the Seller (Smarte Certify™) through the private/public key pair rings and the digital signatures programmed through the application.

Such product offerings that are a part of the MoveMoney™ Smarte™ system include a unified shopping cart (Smarte Shopcart™) that provides the same look and feel across different Seller sites. It also tracks multiple buys across different Seller sites by the same Buyer and group buying of the same product from the same Seller through different Buyers. Multiple currencies are a part of the system and can allow international shopping with security, ease and comfort. Buying patterns are tracked dynamically to allow the Seller to streamline the advertisements during checkout (Smarte Ad™). Banner advertisements at different Seller web locations are made dynamic (Smarte Banner™) to facilitate rapid and instantaneous checkout, rather than a static advertisement that is more a nuisance to the online Buyers.

The Smarte VII™ architecture also ensures security by linking the Buyers and Sellers to the MoveMoney™ system, keeping track of the multiple sessions that are opened and closed during the checkout process. The design allows for automatic encoding of all data using special hashing routines, and encrypting of the same data for security against spoofing. The Smarte

28

VII^{TM} platform keeps tracks of inventory and allows for appropriate and automatic updates to the Seller's inventory system. The application also links to a true B2B (business-to-business) application that can facilitate procurement management and supply-chain management.

Smarte Checkout^{TM} is an application that is programmed in the Sellers' sites as a part of the Smarte VII^{TM} platform installation. Smarte Checkout^{TM} allows the Buyer to checkout products at the Sellers' sites with ease and comfort while being assured of a secure transaction. It also facilitates the Buyer to use multiple payment methods and payment flexibility (Smarte Pay^{TM}) to complete the transactions. The Smarte Checkout^{TM} technology prevents the transfer of sensitive financial information to the Seller, thereby assuring utmost security and confidence to the Buyer. After the Buyer selects the products/service from the unified shopping console at the Sellers' locations, the Buyer is prompted to select the Smarte Checkout^{TM} application for completion of the checkout process. The application requires the electronic profile username and password, in addition to the unique authentication that the Buyer obtained as a part of the signup and profile creation process.

Smarte Checkout^{TM}, working within the Smarte VII^{TM} platform, tracks the entered electronic access information, and retrieves the appropriate profile information. The application waits for the double authentication from the Buyer (Smarte Device^{TM}) and validates the information prior to displaying the profile information. Any changes to the default shipping address, payment type, pay method and shipping method is dynamically updated and adjusted for price through the application. When the Buyer authorizes the transaction, Smarte Checkout^{TM} confirms the transaction and forces the Smarte VII^{TM} platform to update the Seller's database and close the connection to the MoveMoney^{TM} server. Thereafter, the transaction database and the profile database are updated with the transaction information, and appropriate notifications are sent to the Buyers and Sellers. Transactions are tracked for clearing, settlement and returns, and appropriate risk management techniques are applied to facilitate settlement with Buyers and Sellers.

29

Smarte Pay™ is a new and innovative MoveMoney™ payment technology that allows for multiple payment methods and payment flexibility at shopping sites. FIG. 96 depicts elements of the Smarte Pay™ e-payment management platform. It brings the Financial Institutions directly onto the forefront of the online payment processing (Smarte ACH™, Smarte Credit™). Smarte Pay™ also allows for individual loan houses (Smarte Loan™) to participate in the online payment processing. Smarte Cash™ (payments through the MoveMoney™ E-cash account), Smarte ATM™ (payments through the ATM network), Smart Cards (payments through stored value smart cards), E-cash (payments through third party electronic cash alternatives), private label cards (payments through private label cards such as Sears, JC Penny etc.), and credit cards (VISA, MC, Amex, Discover, etc.) are a part of the Smarte Pay™ system.

Smarte Credit™ is an offering that the Financial Institutions promote to their Buyers through the MoveMoney™ system. Smarte Credit™ is a signature loan amount that the Financial Institutions offer to their Buyers, in the event the funds become unavailable to honor their online transactions from their regular checking/savings/overdraft accounts. Smarte Credit™ helps in assuring that the online Sellers are guaranteed the funds to the extent that the Smarte Credit™ amount permits. The Smarte Checkout™ keeps dynamic track of the credit limits, as applied to Buyers and Sub-Buyers, and facilitates the completion of the transaction appropriately.

With Smarte Pay™, Buyers can split pay among various alternatives. Payment flexibility by way of deferred payments further enhances the Buyer's options during the checkout process. Buyers also have the flexibility to assign Sub-Buyers to the account and set appropriate limits to them from among their Smarte Pay™ portfolio.

Smarte Profile™ is an online electronic profile for Financial Institutions, Buyers and Sellers who are a part of the MoveMoney™ system. The 3-dimensional model within the MoveMoney™ data structure allows for each of these entities to be one another, and the system keeps track of appropriate security levels, and permissions to view/edit/delete/archive data. Sellers can have Sub-Sellers, Buyers can have Sub-Buyers and Financial Institutions can have

30

multiple branches within the system. The Smarte Profile™ maintains the appropriate personal profile information as applies to the entity as well as maintains a log of all transactions, messages, notifications, rewards, returns and updates. Sellers can track all transactions from their Buyers, and Buyers can track transactions from their Sellers.

5 Smarte Wireless™ platform parallels the Smarte Checkout™ offering in the area of wireless applications to allow Buyers to purchase products and services through M-commerce (mobile-commerce). The Smarte Wireless™ platform allows for dynamically linking the Buyers through the wireless service providers to the MoveMoney™ system by providing the same value propositions to Buyers, Sellers and the Financial Institutions that the Smarte Checkout™ system

10 provides.

System Structure and Entity Relationships

The Structure of the system inherently allows for expansion and additional complexity, even at the "core" of the system, by introducing the methodology of the "unknown". Using this mentality, wherever there was the possibility of another "type" of anything, should as primary

15 entities, accounts, authentication devices, etc., the structure of the system incorporates the "unknown" type. This methodology for structure requires that should a new "type" of anything be added to the future system, there is no requirement to ever have to go back and "redesign/redefine" the core system. It is simply a matter of adding a single type "code" to an existing data table, and adding additional tables as required, instead of having to essentially

20 redesign the existing system.

At the top level of the hierarchy are the following Primary System (User) Entities:

- Administration (MoveMoney)

- Financial Institutions (Banks)

- Sellers (Merchants)

25 - Buyers (Consumers – Both Retail and Commercial)

- External Authentication Sources

- End Authentication Users

31

These entities are linked by an assigned MoveMoney™ identification initially given to them. Once the MOVEMONEY identification is linked to an entity, that identification carries over to the others if they are created in the system. Each of these entities maintains accounts that will be used for various reasons. As with the primary three entities, the accounts are also given a master identification, with details stored according to the account type. All accounts, regardless of type, are related back to a Financial Institution. In some cases, it is possible that the Financial Institution "sponsoring" the account will also be the same one that "owns" the account.

In addition, each of the System "users" are also maintained separately within the Smarte Authentication™ portion of the system as independent "End Users", allowing them not only access to the Smarte System™, but allows the Smarte Authentication™ portion of the system to function seamlessly with an External Authentication Source NOT incorporating the Smarte Pay™ system.

In reference to FIG. 3, The Smarte System™ is 3-dimensional and horizontal across the various entities Primary System (User) Entities.

Financial Institutions includes such entities as Banks, loan companies, credit unions, e-cash merchants, and MoveMoney™ itself. Financial Institutions have individual Users, which can manage the functions and requirements of the System. The relationships between the Financial Institution and other directly related entities within the System are displayed in FIG. 4.

Sellers are not only merchants with hard products to sell, but can also be service organizations. Sellers may also select to utilize an external system, with access for Buyers via the Smarte VII™ platform, or utilize the Smarte™ system inventory itself. The structure for Sellers is similar to Buyers in that a parent Seller can be specified, and to roll-up" transactions from multiple "related" Sellers. Parent/Child relationships for Sellers can be "Prime/Sub" in the manner that they eventually can be with the Buyers. The Seller profile contains the basic information about the Seller, names, and attributes. It serves as the "hub" for all seller activities and specific information. The Seller has the capability to enter "blocks", in the form of Buyer accounts and account numbers. Blocks entered at the Seller level remain at the Seller level and

32

are not applicable to other Sellers. Sellers, like Financial Institutions, have individual users that have access to the system in order to manage product information and other related entities. The relationships between the Financial Institution and other directly related entities within the System are displayed in FIG. 5.

5   The next entity within the Smarte^{TM} System is that of Buyers. There are rules/considerations regarding Buyers within the structure:

- Buyers are not only the typical retail consumer. They may also be part of a Seller organization in the manner of a purchasing agent.

- Buyers may be prime or sub type buyers.

10   - Buyers can maintain multiple accounts that can belong to the same Financial Institution.

- Buyers can maintain multiple accounts that can belong to a different Financial Institution.

- Multiple Buyers may use the same account, with varying authorizations and limits, however the Smarte System^{TM} treats these multiple uses as individual accounts.

15   - Buyers must belong to the Smarte^{TM} system in order to process transactions through the Smarte Checkout^{TM} system.

Buyers are structured so that a Prime Buyer can exist, with controlled Subordinate Buyers under it. Examples of this in practical applications would be a parent authorizing their child to use their account to purchase items over the Internet, while at the same time limiting the amount

20   that they are authorized to use from the account over a specific time frame. Another example of this as a practical application would be an employer (as the Prime), authorizing the purchasing agents under it to use the company's account to purchase supplies over the Internet, again, limiting/controlling the authorizations. Authorizations issued from primes to Sub Buyers can never exceed the amount authorized to the Prime, nor can the total purchases for all of the Sub

25   Sellers (including the Prime) ever exceed the amount that the prime Buyer is authorized for over a given time period.

33

Commericial Buyers are treated in a similar fashion as Sellers and Financial Institutions within the system, in that since they are considered to be an organization rather than an individual person, they have individual users, while a Retail Buyer is considered to be a single individual, and therefore the retail buyer is also the individual user within the system. The relationships between the Financial Institution and other directly related entities within the System are displayed in FIG. 6. The relationships between the Retail Buyers and other directly related entities within the System are displayed in FIG. 7.

Administration Users are the MoveMoney™ system personnel. Special access and privileges are granted to Administration users in order to maintain the system and information as required. Administrative personnel are also delineated in their access privileges by having a limited number of trusted personnel granted Security Officer status capability. When in this "mode", the Administrative User can perform "system level" maintenance not available to other Administrative personnel.

Sellers and FI's, in order to interface within the Smarte System™, as well as utilize the Smarte Authentication™ System, must also be External Authentication Sources. MoveMoney™ itself is an External Authentication Source to the System in order to control Access to the Smarte System™. It is not a requirement for a business to be part of the Smarte Pay™ system in order for them to utilize the Smarte Authentication™ portion of the system, as it is designed to also work independently of the Smarte System™ itself. The relationships between the External Authentication Sources and other directly related entities within the System are displayed in FIG. 8.

In order for Access to any portion of the Smarte System™ to be granted to an individual user, they must be recorded in the system as End Authentication Users. End Users (to whom devices have been issued) maintain no implicit direct access within the Smarte System™, unless entering as an authorized user into the system via the access granted via the standard Plugin. Therefore, no special access area exists for them. End Users are maintained at two distinct levels within the Smarte System™. The first level is the "common", or system level, to which each of

34

the End Users are assigned a unique System Identifier, that identifies the Individual, independent of membership or External Source References (including the Smarte System[TM] itself). No personal information is retained for the End User at this level. The second level is at the level of External Source and External Source End User Reference (i.e.: Login Name) for the particular

5   External Source. This structure allows an individual to be identified, as well as maintain multiple devices across many different external sources where End User's login name/identifier may be different for each of the external sources. Since a Smarte Device [TM] is assigned to the System Level, rather than at the external source level, it allows devices to be utilized across multiple External Sources.

10   At the next level of the hierarchy are the following Primary System (Non-User) Entities.

Attached to the Sellers is a "theoretical" entity entitled "Product Class". The relationships between a Product Class and other directly related entities within the System are displayed in FIG. 5. This entity serves multiple functions:

- Enables Sellers to segregate and differentiate particular groups of inventory or services.

15   - Enables risk to be assessed separately for individual Seller product lines or services.

- Enables fees and reserves to be managed separately for individual Seller products lines or services.

- Enables risk to be assessed separately for individual Seller product lines or services.

- Enables fees and reserves to be managed separately for individual Seller products lines

20   or services.

- Enables the Seller to identify different shipping and payment limitations/requirements for individual product lines or services.

- Enables tax schedules to be managed separately for individual Seller products lines or services.

25   Under the Product Class are the Products themselves. A product can be either a physical product or a service provided by the Seller. Products also can maintain specific requirements as

35

placed on them by the Sellers. The relationships between a Product and other directly related entities within the System are displayed in FIG. 5.

All Product Classes and Products maintain a "sub-entity" referred to as Categories. The relationships between a Category and other directly related entities within the System are displayed in FIG. 5.The Categories serve the following functions:

- Serves to identify product classes and products to a "type" of product or service.

- Provides a means of readily searching for a particular "group" or type of product/service.

The system maintains a variety of Accounts. Accounts maintain separate requirements for the three primary entities as well. All of the primary entities within the Smarte™ system are required to maintain at least ONE account, with the additional requirement of Financial Institutions and Sellers being that at least one account must be a "Bank" sponsored ACH accessible account type. Payments through various account types are handled according to their individual or specific processing requirements. The relationships between accounts and other directly related entities within the System are displayed in the following Figures: FIG. 4 for Financial Institutions; FIG. 5 for Sellers; FIG. 6 for Commercial Buyers; and FIG. 7 for Retail Buyers. The relationship between accounts and External Authentication Sources is the same as that between Sellers and Accounts.

There are multiple types of accounts that the system maintains. Again, the structure of the system is designed so that the addition of a new "type" of account does not require a major changes to existing tables or structure. Each Different Type of account added to the system requires that additional coding be added in order to handle the processing for these types of accounts, however the addition of a new "type" of accounts. Accounts and the subsequent processing are discussed in detail later in this document.

Account Format Validation is performed by the Smarte System™ in that the "formats" for accounts are maintained in order to help reduce the potential for data entry errors. Some of the most common entry errors that occur, especially on longer account numbers, is either

36

entering two many digits (duplication of a number or series of digits/characters), or missing a digit/character in the entry. What the format checker does is create a "template", or mask that can be used to validate account numbers that are entered into the system. It does this through a set of predefined characters.

The following are examples or account numbers and the resulting "mask":

'01560456144567892'   'CY764533'   '578-GH-6738233D'

'#################'   'XX#######'   '###-XX-#######X'

These validations are maintained at the level of Financial Institution AND Account Type. The account Format Checker is NOT designed to BLOCK/STOP an account# from being entered incorrectly, only flag the USER to the potential for the account number to be invalid. In this manner, it helps to identify mistakes to the user. The way that the validation takes place, is that the FIRST time an account number is entered into the system for a specific Financial Institution, the template is created for that account number and stored. The NEXT time an account number is entered against that Particular FI, the system converts the entered number to a mask and validates against the stored mask. If more than ONE formats are stored for that particular FI, than the created mask for the entered account number is verified against ALL existing for the FI to see if there is a match. If NO MATCH is found, then the USER is given a warning that the account number entered appears to be invalid. The option to override and save the format as valid is given to the user, as well as override but NOT save.

Example:

Stored Mask for FI: '#################'

Teller Enters: '8924314566666418'

This is converted to: '#################'

Stored Mask(s) retrieved and found that they do not match:

'#################'(Stored)

'#################' (Entered)

37

Warning is given to USER at this time. In this example, the user "missed" a digit, a common error. Since we have no way to predict the number of potential account formats/lengths/patterns, etc., this type of check is utilized.

Orders are the collection of all information processed when a Buyer performs a purchase though the Smarte™ system. The individual components of an Order are Line Items and Transactions.

Within each order, each individual "purchased" item or service is considered a separate Line Item. Lines Items are maintained independent of the Account types, as well as the subsequent required transactions.

Transactions are an entity in that they are grouped not only under the Order, but also in "Batches", which are used to calculate and maintain commissions and fee amounts to other entities. Transactions also maintain all of the specific account information. Where the Buyer has utilized a "split-payment" option, there will be one transaction for each account used within the Order. Transactions are maintained at two levels, common transaction information as well as information specific to the type of account utilized. Also grouped under an Order (at the individual transaction level) are any "returns" that occur against any of the transactions under that individual order.

Transactions can also exist within the system without being attached to an Order. Since the Smarte System™ is not limited to solely an "order" system, there are additional mechanisms outside of an order that can trigger a transaction, such as a commission payment to a Financial Institution via the system, or a Buyer initiated transfer of funds between accounts. In addition to this, the transaction generation process itself can trigger additional transactions of the same as well as other types to also be generated, depending on account, transaction, and type of action being processed.

Access to the system is granted to End Users via a Device. Devices are initially maintained maintained by the system in an "inventory", and are grouped sequentially by "Lots". Devices are placed into inventory via manual entry, or import of information from a generated

38

import file where the devices have been serialized with a serial number string internally. These devices are issued from inventory to External Sources, for subsequent distribution to End Users. MoveMoney™ is itself an External Source in this regard as part of the authentication requirements for the Smarte System™. This relationship is displayed in FIG. 9.

5   Access Authorizations are the "rules" defined by the external source for particular access to a single site. There are mechanisms within the system that allow for the External Source to dynamically have a single Authorization that can function across multiple access points. In addition, the system is structured to allow a "parent-child" relationship, under which a single authorization can maintain a single processing set of rules, while other specific requirements can

10   be defined under different "child" authorizations, allowing the External Source to call the "parent" authorization, while assigning the individual "children" authorizations to the specific devices as needed. An example of this application would be where access is limited to specific time periods during the day based on a worker's daily shift, and there are three working shifts. Under this scenario, the External Source need set-up and reference only the parent, but can then

15   create and assign an unlimited number of "children", each one limiting the access time based on shift, to the individual End Users as required. Authorizations "rules" are essentially split into two categories: Functional and End User Access.

       Functional Authorization Rules define how the Authorization functions, and directs the plug-in on the External Source Server in how to react to authorization requests. Functional rules

20   include:

        - SOURCE URL FROM WHICH ACCESS AUTHORIZATION REQUEST
        ORIGINATES
        - Single Character Code indicating Base Type of Authorization Application: "U" – User
        Authentication; "P" – Product Authentication

25   - URL to Pass to Upon Acceptance of Authorization
        - URL to Pass to Upon Rejection of Authorization

39

- URL to Pass to Upon NOT Found Result (Excludes where Not Found has resulted in Rejection

- Static String to Pass to URL Upon Acceptance of Authorization

- Static String to Pass to URL Upon Rejection of Authorization

- Static String to Pass to URL Upon NOT Found Result (Excludes where Not Found has resulted in Rejection)

- Single Character Code indicating TYPE of Implementation regarding the SA System Universal Password.

"N" – None – Universal Password is NOT accepted. This is also the applicable code utilized where a NO password and/or No login access system is utilized. Source Login/Password Combination as acceptance ONLY

"R" – Universal Password REPLACES the Source's Password. The information entered into the Source's password field in the login screen is passed directly to the SA system for primary validation of password.

"S" – Supplemental: The Universal Password is utilized as a secondary password, which can be used as an ALTERNATE to the source's OWN maintained password.

"X" – Indicates that Source system does not REQUIRE or USE a Password at all for THIS authorization. Primary utilization is confirmation points internally within the system, NOT as a primary login/access use.

- Single Character Code indicating WHAT type of ACTION is taken upon determination of the acceptance/Rejection Criteria

"P" – Plugin handles subsequent Action based on Acceptance/Rejection Criteria.

"S" – Source handles action based on results passes back by the SA system

- APPLICABLE ONLY IF SAF0225 is "P": Single Character Code indicating Type of Passed String Handling to occur

"D" – Dynamic Strings Passed to Plugin

"S" – Static Strings utilized by Plugin – Stored

40

- Perform Anti-Piracy Validation of Device (where applicable)? "Y" – Yes; "N" – No

End User Access Rules define what limits, if any, are placed on the End User's Access. In addition to these being set at the "master" authorization level itself, these rules can also be altered or adjusted for each individual device, providing a means for overriding specific values for individuals. End User Access Rules Also apply to the realm of Product Authorization, and are maintained in the same area within the system, as for the purposes of structure, in Product Authentication, the Product Itself is considered to be the End User. End User Access rules include:

- Is Access Controlled on Time Basis? (Y/N) (Pertains primarily, but not limited to USER type Authorization)

- Contains Beginning Available Access Time for User (Applicable only if Time Lock = "Y")

(Pertains primarily, but not limited to USER type Authorization)

- Contains Ending Available Access Time for User (Applicable only if Time Lock = "Y")

(Pertains primarily, but not limited to USER type Authorization)

- Is Access Controlled on Periodic Basis? (Y/N) (Pertains primarily, but not limited to PRODUCT type Authorization)

- Total Number of Times per DAY that Access for single DEVICE is granted. NOTE: ACCESS BASED ON DEVICE, NOT USER. (Pertains primarily, but not limited to PRODUCT type Authorization)

- Total Number of Times per WEEK that Access for single DEVICE is granted. NOTE: ACCESS BASED ON DEVICE, NOT USER. (Pertains primarily, but not limited to PRODUCT type Authorization)

- Total Number of Times per MONTH that Access for single DEVICE is granted. NOTE: ACCESS BASED ON DEVICE, NOT USER. (Pertains primarily, but not limited to PRODUCT type Authorization)

41

- Total Number of Times per YEAR that Access for single DEVICE is granted. NOTE: ACCESS BASED ON DEVICE, NOT USER. (Pertains primarily, but not limited to PRODUCT type Authorization)

- Total Number of Times DURING THE LIFE OF THE AUTHORIZATION that Access for single DEVICE is granted. NOTE: ACCESS BASED ON DEVICE, NOT USER. (Pertains primarily, but not limited to PRODUCT type Authorization)

- # of DAYS from COMBINATION of: Device Assigned to User (Activated) AND Auth Assigned to Device that: AUTHORIZATION Assigned to Device Expires. AUTO_EXP_DATE. Note: There is No Upper Limit on the Number of DAYS that can be entered, other than the INTEGER Maximum Value itself. Note also that a NULL or ZERO Value in this field indicates NO AUTOMATIC AUTHORIZATION EXPIRATION.

- Individual Days of the Week that Access Is granted

The attachment of the Authorization itself, combined with any specific override settings, are used to create an individual Access Authorization entity, unique to each device. This relationship (for End Users) is shown in FIG. 10. The basic relationship of these authorizations in regards to Product Authentication is shown in FIG. 11.

The purpose of maintaining LEGAL "Bank" Holidays within the Smarte System^{TM} is to prevent excessive "premium" charges from being levied against MoveMoney^{TM} by the Federal Reserve. The EFFECTIVE DATE for transactions, therefore, is calculated as the NEXT Working day following the transaction generation. By default, Saturdays and Sundays are NOT considered to be "working days". Holidays within the system as well, are considered to be "non-working" days. The ONLY holidays that are to be maintained within the system, are those days that are considered "bank" holidays. Example: If ACH transaction processed on Thursday, Effective date would be the next day: Friday. Example: If ACH transaction processed on Friday, Effective date would be the following MONDAY. Example: If ACH transaction processed on

42

Friday and the following MONDAY is a HOLIDAY, then Effective date would be the following TUESDAY.

SYSTEM SCREENS AND USER INFORMATION REQUIREMENTS

The Smarte System™ is divided "functionally" into two separate areas at this time. The first is Smarte Authentication™, and the second is referred to as Smarte Pay™. This is done as while the Smarte Authentication™ portion of the system is part of the Smarte System™ itself, MoveMoney™ must itself act as an "external" entity in order to set up and maintain access rights for the Smarte System™ using the functions of the Smarte Authentication™ section. In this manner, there is only a single hardened security and access methodology employed in accessing not only the Smarte System™, but External Source sites as well. This prevents having multiple "weaker" systems filled with exceptions that must be maintained to "allow for" the Smarte System™ itself.

Each Individual Screen within the Smarte Authentication ™ portion of the system is identified by a screen "identification code", the placement is as shown in FIG. 12. If specific Screens are "duplicated" for different purposes, that the applicable screen designations will remain, however the individual variants of these screens will be followed by an alpha character (A, B, C, etc.) in order to identify the individual variants. Note that this does NOT apply to variations within the SAME form itself, only where these forms are PHYSICALLY separate.

Edit Checks are considered those validations of information that can be performed in regards to themselves, such as is the item a valid "state" or postal code; is a mandatory information entry field left blank, is an entered identification number the correct length and format, etc. These also include validations that can be performed within the same form/data table itself, such as a "date started" could not be entered after a "date ended".

Guardians refer to validations that must be cross checked against multiple forms or data tables, and include protection against the entry of duplicated records, or records containing information that conflicts with other records or information limitations already in the system. Standard Validations for information within the system is as follows:

43

Global

- Regardless of other checks, all information requirement checks for data are performed at the RECORD level. Additional field level checks may be performed, but are ALWAYS duplicated at the record level. All text fields that require specific data (specific characters) will be coded using the standard text convention to block entry of invalid characters.

- Individual Situations and requirements may be applicable to a specific circumstance or particular application where the need to over-ride the standard information edit checks and guardians apply. The following information in this section regarding "standards" is given as a reference only, and is intended to serve as a programming guideline, where such requirements are not implicitly stated elsewhere.

- Names
  - Full Name; Short Name; Contact Person; First Name; Last Name
    - Alphanumeric (a-z, A-Z, 0-9)
    - Spaces
    - Extended Characters like & (ampersand) . (dot) , (comma) - (hyphen) * (asterisk) ' (Single quote)
  - Middle Initial
    - Always Optional
    - Single Alpha-numeric Character
    - Extended Characters NOT permitted
  - Name Prefix
    - Alphanumeric (a-z, A-Z, 0-9)
    - No Spaces
    - Extended Character: . (dot)
    - Requirement varies with individual application

44

- Name Suffix
  - Alphanumeric (a-z, A-Z, 0-9)
  - No Spaces
  - Extended Character: . (dot)
  - Always an Optional Requirement
- Addresses
  - 2 lines of 30 characters each are always given for "street address" portion. Information can not exist on the second line if the first line is blank. Rather than error, the program will always shift the second line to the first, then clearing the second line.
  - Spaces and Extended Characters are allowed in the Street Address Lines.
  - for Cities, Spaces and Extended Characters are allowed.
  - Where the 5 digit zip code is optional, if any portion of it is entered, it must be 5 digit numeric, or made blank.
  - The 4 digit extension on a Zip Code can not exist without the 5 digit portion being entered. The four digit zip code extension is ALWAYS optional.
  - "State" must conform to a valid 2 character Postal Code.
  - Email
    - Alphanumeric (a-z,A-Z,0-9)
    - Special Characters like _ (Underscore) - (hyphen) . (dot) ~ (tilde) ' (Single quote) @ (at the rate)
    - Format:
      Before @ Symbol:
      First and Last Character should be Alphanumeric and Special Character can be in-between them
      After @ Symbol:

45

First and Last Character should be Alphanumeric and Special

Character can be in-between them. At least one . (dot) should be in-between First and Last Character

5

e.g.:

move-money@elmaq-software.com

move money-elmaq@mmc-inc.com

- Web Page

  - Alphanumeric (a-z, A-Z, 0-9)

10

  - Special Characters like . (dot) _ (Underscore) - (hyphen)

  - Format:

    a.b.c

    a – www

    b – First and Last Character should be Alphanumeric and special Characters can be in-between them

15

    c – Alphanumeric

    e.g.

    www.movemoney.com

    www.usa.net

20

- Telephone Numbers (includes Fax, Modem, Cell, etc.):

  - Phone Numbers are always divided into 3 separate text fields on the screens. Where a phone # is optional, if any portion of the phone number is entered, the entire number must be entered correctly. Area Codes are always required if a phone # is entered.

25

  - Alpha Characters are NOT accepted in the phone number fields.

46

- Where a telephone# extension field is given, the extension can not be entered unless a valid phone number exists applicable to that Phone Extension.

- Dates:

- All dates entered must be valid (1/1/999 through 12/31/9999).

- All dates that relate to other dates (such as "start" and "end" dates) are validated against each other (example: End date can not be before Start Date).

- Dates are entered and maintained in the system in DD/MM/YYYY format.

- Where Dates are presented on the screen in the form of a selection, the "default" date presented must be "intelligent to the individual application for that/those field(s).

- RTN's (Routing Transit Number)

- All Entered RTN's must be 9 numeric characters in length.

- All RTN's entered must validate through a global RTN digit check.

- RTN can NOT be "000000000", even though this DOES pass the Digit Check.

- SSI#'s

- Social Security Numbers MUST be either 9 numeric characters or 8 numeric characters with an alpha character (A-Z) in the 9th position. (This accounts for special CA based Medi-Cal Situations encountered)

- Bank Account #'s

- Bank Account #'s must process through the Global Account # Format. Note that failed check does NOT prevent entry of account#, only issues a WARNING to the user to reevaluate the entry.

- Amounts

- Integer Amount

47

-      Numeric (0-9)

-      Size dependant on individual application

-      Currency/Fixed (2 Decimal Places)

-      Numeric (0-9, and ".")

5   -   Format:

        Max 16 Characters

        Max 13 Numbers before . (dot)

        2 Numbers after . (dot) (padded with zeroes as/if required

        As Displayed:

10   -   Currency Symbol Precedes Value

-      Percentage

-      Numeric (0-9, and ".")

-      Format:

        Max 6 Characters

        Max 3 Characters before . (dot)

15   Max 2 Characters after . (dot)

        Value should be <= 100.00

        As Displayed (without Label Reference to Value "type"):

        -      "%" Follows Value

20   External Source Profiles

-      Mandatory Information:

        Names (both full and abbreviated)

        Date established as "Company/Corporation"

        Plugin Use Type Code

25   "S": User Auth – Single Device/Type

        "M" - User Auth – Multiple Devices/Types

        "P" – Product Authentication

48

"C" - Combination

Sales or Service Category

Address/Contact Information

External Source Accounts

5 - Must be attached to a Specific External Source

- Must be attached to a Bank

- Account Number SHOULD pass Account# Format Check

- RTN/Account DOES NOT HAVE TO BE unique within the system

- Mandatory Information:

10 Type of Account (Checking/Savings)

Actual Name(s) on the Account

- Applicable Account Types:

Checking

Savings

15 Admin

External Source System Users

- Mandatory Information:

Names (First/Last)

Login Information (Login Name/Password)

20 Sales or Service Category

Address/Contact Information

Devices

- Only Devices as defined by the SA system itself may be utilized within the System

25 - A Device May be declared to be "blocked" from Cross Utilization. In this event, the following applies:

49

- Device Control resides with the Issuing External Source (as well as Admin)

- Devices are "invisible" to other External Sources, as are attached Authorizations.

5 - Only Devices that have this condition can be "killed" by the issuing external source.

- Devices NOT blocked from cross utilization can not be "Killed" by ANY external source. The action to "Kill" a device results in only the removal of ALL Authorizations previously granted by the External Source attempting to "Kill" the

10 device. ONLY MoveMoney™ Administration can "Kill" a cross utilization capable device.

Lots

- Lots must be retained in a complete "sequential" series.

- Lots can not cross device types

15 - Lots are to be "split" by the system as needed in order to maintain the sequential series

- In the case of a split required, the low end of the Lot series will retain the original lot designation, and a new lot designation will be applied to that portion of the series following the split.

20 Device Ownership

- For an External Source, Device Ownership is defined as having both Complete Device Control Authority and the ability to Transfer that Complete Device Control Authority to another External Source.

- Device Ownership originally resides with Inventory.

25 - Issuing a Device to an External Source from Inventory places the Device Ownership with that External Source.

50

- Once an External Source holds Device Ownership, that External Source can Transfer Device Ownership to another External Source.
- Device Ownership can be held by one and only one External Source.
- An External Source retaining Device Ownership can grant some or all Device Control Authority to another External Source while still holding Device Ownership.

Device Control Authority

- Device Control Authority is a set of device management rights including Device Activation, Authorization Attachment, Authorization Removal, and Access Usage Override.
- The External Source holding Device Ownership can grant any or all device management rights encompassed by Device Control Authority to other External Sources.
- Complete Device Control Authority is conferred when Device Ownership is Transferred from one External Source to another External Source.
- Complete Device Control Authority can be held by more than one External Source, provided the External Source holding Device Ownership grants Complete Device Control Authority to another External Source.
- If an External Source Transfers Device Ownership, then any Device Control Authority it had granted prior to the Transfer is removed.
- Not until Device Ownership is Transferred by an External Source can it give up Complete Device Control Authority.
- Device Control Authority can NOT be extended beyond a Single Level of authority.

Financial Institutions

- Bank Name Required (14 Characters for ACH)
- Valid RTN Required for Banks (must pass RTN digit checks)

51

- RTN must be Unique within the system.
- Financial Institutions Address and Standard Telephone Number are Optional IF NOT a sponsoring entity

Sellers/Merchants

- Transaction Information Requirements must be specified, noting that any requirements specified at the Seller Level are automatically "locked" at the Product Class Level for the individual Sellers.
- Mandatory Information:

  Names (both full and abbreviated)

  Date established as "Company/Corporation"

  Initial "Risk Assessment" (A or B)

  Sales or Service Category

Seller Accounts

- Must be attached to Seller
- Must be attached to a Bank
- Account Number SHOULD pass Account# Format Check
- RTN/Account must be unique within the system
- Mandatory Information:

  Type of Account (Checking/Savings)

  Actual Name(s) on the Account

Product Classes

- Product Classes must be originated from MOVEMONEY. The Sellers have full viewing capability, but little control over them.
- Must be attached to a Seller.
- Requires that a Seller Account be attached.

52

- Transaction Information Requirements must be specified, noting that any requirements specified at the Seller Level are automatically "locked" at the Product Class Level for the individual Sellers.
- Mandatory Information:
  - Product Class Description (Full and Abbreviated)
  - Sales or Service Category
  - # of Days to Delay NSF Fee Transaction
  - Min/Max amounts required for individual Transactions
  - Reserve and Fee Type/Amounts

Products

- Must be attached to a Product Class
- "Sale" Amount for products can not exceed Product Class Minimum or Maximum Amounts.
- Mandatory Information: [Not Applicable to Phase I Implementation]
  - Product Description (Full and Abbreviated)
  - Sales or Service Category
  - # of Days to Fulfill Product/Service
  - Provided by Seller/Other
  - Default Charge for Product/Service
  - Min/Max amounts required for individual Transactions

Buyers

- Must be designated as either Commercial or Retail
- General Mandatory Information:
  - Buyer Address
  - Driver's License State of Issue (required only if D/L# Entered). Can NOT be entered by itself without D/L # being entered as well. Not applicable to Commercial Type Buyers.

53

- Commercial Type Specific Mandatory Information:

    Company Name

- Retail Type Specific Mandatory Information:

    First/Last Name

5   Buyer Accounts

- Must be attached to a Buyer

- Must be attached to a Financial Institution

- Account Number SHOULD pass Account# Format Check.

- Mandatory Information:

10   Type of Account (Checking/Savings)

    Actual Name(s) on the Account

    - Mandatory Information IF Co-Signer on Account:

        - Co-Signer Name

        - Co-Signer SSI#

15   - Co-Signer Address

        - Co-Signer Telephone Number

Holidays

- Must be a valid date.

- Duplication of Dates for various Holidays MAY be added provided names are not

20   the same for two

    separate entries on the same date.

Standard System (Flow) Guardians

- At Buyer Sign-in following Successful Log-In:

    - Parent/Primary Buyer

25   - Has Buyer Activity Been Suspended?

        - If so:

54

- Notification to Buyer of this, origin of block, reason for Block, whom to contact.
- No further access allowed – Returned to main (unsecured) page, or Seller's Web Site (if via Smarte VII™ system interfaces)

- Sub- Buyer
  - Has Buyer Activity Been Suspended?
    - If so, is due to Parent Buyer being locked?:
      - If Parent Buyer Locked:
        o Notification to Buyer of this, origin of block, reason for Block, whom to contact.
        o No further access allowed – Returned to main (unsecured) page, or Seller's Web Site (if via Smarte VII™ system interfaces)
      - If locked by Patent Buyer:
        o Notification to Buyer of this, origin of block, reason for Block, whom to contact.
        o No further access allowed – Returned to main (unsecured) page, or Seller's Web Site (if via Smarte VII™ system interfaces)

- All Buyers
  - If Critical Activity (new), then option is displayed as RED Blinking Option.
    - Critical Activity consists of the following for Buyers:
      - Activity Triggers
      - Account (Individual) Locked
      - Return

55

- Smarte Credit™ Activation
- NSF Fee Transaction

- Prior to "Shopping" (Buyer):

  ▪ Does Buyer have accounts with available balance?

    - If not, inform Buyer that they are unable to shop at this time due to..."

- At "Check-out" (Buyer):

  [Note: If multiple Sellers or Product Classes Involved, Guardians must be applied/occur for each related item(s)]

  ▪ Does Seller Permit "Non-Guarenteed" Funds for each Product Class involved?

    - If NO, Does Buyer have Smarte Cash™ Account with sufficient Balance to cover purchase (including additional anticipated amount to cover tax/shipping)?

      o If NO, display "potential unable to complete purchase due to..." message to Buyer.

  - Buyer then selects/adds Shipping Addresses

  - Does Seller Service/ship to selected area for all Product Classes Involved?

    o If NOT, then notify Buyer of which Products/services are in conflict.

Payment Mechanism Selection Screen (Buyer)

- Prior to Display:

  o Retrieve Buyer Accounts

  o Check for Locked Status for each account

  o Check "availability" DB for record

56

- If Record found, display available amount for that account, as the less of:
  - Current Availability amount
  - Current Account Balance (if applicable)
- If Record NOT found, display Current Account Balance if applicable, otherwise, display "N/A"
  - Amounts "available" from the individual accounts displayed on the payment method screen. Locked accounts are ALSO displayed, but user is prevented from using them. Closed accounts are NOT to be displayed.
  - Buyer selects payment mechanisms from display, which includes a dynamic calculator , displaying remaining amount to account for in purchase.
  - Based on previous guardian checks, minimum amounts to be assigned to Smarte Cash^{TM} (or other "Guaranteed" types of accounts) to be shown to Buyer
  - Amounts entered must also fulfill previous guardians listed
  - Amounts can not exceed amount availability where applicable.

Shipment Limitations
- Shipments can NOT be split within a single Buyer Order.
- Shipments must be acceptable based on Seller shipping blocks for those items under each INDIVIDUAL Seller only. Each Seller's products are to be verified against the blocks of the individual Seller only, NOT globally across all line items on the Buyer's order.

SYSTEM SCREENS AND USER INTERFACE

Menus provide the primary navigation for actions to be taken from the screens within the Smarte System^{TM} for the system users, regardless of user type. The following is the basic menu structure for the various users within the system:

57

Sign Up (Common)

    Sign Up Links Page

    Sign Up Financial Institution

    Sign Up Seller

5   Sign Up Commercial Buyer

    Sign Up Retail Buyer

Help (Common)

Forum (Common)

FAQs (Common)

10   Financial Institution Log in

    Administration

        User Admin

            Blocking

                Activity Blocking

15   Account Blocking

        Activity

            Suspend Activity

            Suspend Accounts

        Transaction

20   Smarte ACH™

            Smarte Cash™

            Smarte Credit™

        Refer Merchant

        Identifiers

25   Manage

            New

        Buyer

Add

Buyer

Account

Manage Profile

5   Accounts

Manage Accounts

New Account

Fees And Commission

Manage Fees And Commission

10   New Fees & Commission

Notifications

Manage Notification

New Notification

Blocking

15   Activity Blocking

Account Blocking

Sub Buyer

Identifiers

Manage

20   New

Smarte Credit^{TM}

Activate

Pay down

Reports

25   Seller Log in

Administration

User Admin

59

Critical Activity

Suspend Activity

Inventory

Add

5   Product

Tax Structure

Shipping Details

Shipping Blocks

Manage

10   Product Class

Products

Related Products

Tax Structure

Shipping Methods

15   Shipping Method Limits

Shipping Location Limits

Upload Image

Reports

Buyer Login

20   Administration

Profile

User Admin **Commercial Buyer Super User

Critical Activity

Suspend My Activity

25   Suspend My Account

Shipping Profiles

Sub Buyer **Retail Buyer who can have Sub Buyers

60

Profile Maintenance

Manage Accounts

Activity Blocking

Account Locking

5   Manage Access Blocks

Accounts

Pay Down Smarte Credit^{TM}

Increase Smarte Cash^{TM}

External Source Login

10   Manage [Super User Access Only]

Authorizations Master

System User Admin

View Profile

Devices

15   Transfer

Assign

Granted Device Control Authority

Activate

Access Authorizations

20   Mass Auth Assignment

End User

Add

Edit Profile

Reports

25   Admin Login

Financial Institution

Add

61

Profile

Accounts

Manage

Profiles

5 Accounts

Fees/comms

User Admin

Identifiers

Activity Blocking

10 Account Blocking

Forgot Password

Notifications

Seller

Add

Profile

15 Accounts

Product Class

Manage

Profiles

20 Accounts

Fees/comms

User Admin

Identifiers

Activity Blocking

25 Account Blocking

Tax Structure

Shipping Methods

62

Shipping Blocks

Shipping Method Limits

Shipping Location Limits

Forgot Password

5   Notifications

Product Class

Buyer

Manage Profile

Add Accounts

10   Manage Accounts

Fees/comms

Commercial Buyer User Admin

Retail Sub-Buyers

Identifiers

15   Activity Blocking

Account Blocking

Forgot Password

Notifications

ISO

20   Add

Profile

Accounts

Manage

Profile

25

Fees/comms

Administration

63

Users

Edit

Identifiers

5   User Registration Details

External Source

Add

Profile

Account

10   External Source System Users

Manage

Edit Profile

Accounts

Blocking

15   System User Activity

Accounts

Fees/Comms

External Source System Users

Devices

20

Add

Manual Entry

Import

Manage

25   Issue / Transfer

Granted Device Control Authority

Activate

64

Assign

Access Authorizations

Mass Auth Assignment

End Users

5   Add End User

Import End User

Edit End User

Reports

New Members

10   Security Officer (Available to Select Users Only)

New Account

Manage Accounts

General Parameters

Identifiers

15   Product Categories

Shipping Methods

Holidays

Remove External Source

SYSTEM SCREENS AND LAYOUT

20   Screen Style ("Look and "Feel") is maintained consistent throughout the system. All

Screens maintains the Current System User's Login Name in the upper left hand corner

For the purpose of clarity, all Authentication Specific "Screens" have been given

designations, which is visibly added to each of the screens in the lower left hand corner, for each

of reference, not only during programming, but for ease of reference on behalf of customer

25   service applications as well. This is as shown in Fig. 12. Where specific Screens are "duplicated"

for different purposes the applicable screen designations will remain, however the individual

variants of these screens will be followed by an alpha character (A, B, C, etc.) in order to identify

65

the individual variants. Note that this does NOT apply to variations within the SAME form itself, only where these forms are PHYSICALLY separate.

The Main/Home Screen Layout is displayed in FIG. 13. These are the options available to the user in the "unsecured" portion of the MoveMoney™ System (i.e.: no log in required). Entry #1 defines the home page of the system. This is the screen where all users (other than MoveMoney™ administration) are first presented with. This page also provides access to all "unsecured", or non-member services/options, as well as log-in access for members. The basic areas are as follows:

- Feedback contains an area where the user (member/non member) can enter comments regarding the site in general. Responses are made available to MoveMoney™ personnel via email.

- About us is the area of the system that tells about our company and the people within it. This area may contain additional screens below it as needed (not shown in diagram).

- FAQ's: A screen where Frequently Asked Questions and Answers to those questions are displayed.

- Press: Information Page that contains recent news items pertaining to MoveMoney™.

- Demos: From this screen, the users can access demonstration portions of the system designed to give overviews of the system.

- Downloads: From this screen, the users can download files that MoveMoney™ have made available to "the general public" regarding the Smarte System™. Files may be technical briefs, FAQ files, Powerpoint (or other format) presentations, etc.

- Careers: This screen allows the user to email MoveMoney™ in regards to employment opportunities listed on the page.

66

- Contact Us: This is a simple display page that lists the various means to contact MoveMoney™ / MoveMoney™ personnel.

- Services: An Information screen regarding products/services available from MoveMoney™.

- Subscriptions: Information regarding MoveMoney™ PAID information and subscription services.

- Sign-up: This screen allows the user the opportunity to select the type of member the user would want to sign-up as.

- Buyer: User enters basic Buyer profile and contact information on this screen.

- Seller: User enters basic Seller profile and contact information on this screen.

- Financial Institution: User enters basic F/I profile and contact information on this screen.

- Log-In: In this screen, the user enters Log-in name and password.

  o Device Handling: This screen appears, specific to the type of physical verification device that the user has been assigned. If the user has instead locked the ID to the particular machine, the alternate screen is utilized instead only if the user is downloading the "key" for the first time.

  (or)

  o 1st Time Download: This screen allows a NEW user to download an encrypted algorithmic key to their individual computer on a one time basis, thereby locking their access as a member to the MoveMoney™ system to a single machine.

- Financial Institution/Seller/Buyer (Main): These are the initial screens with options that the users are presented with when log-in has been successful. Since a user may be more than one primary entity types, they are allowed to switch between "modes" of use, depending on accessibility.

67

The main Screen layout for the Financial Institution User is displayed in FIG. 14. The basic areas are as follows:

- Financial Institution (Main): Primary entry/option screen for members functioning in the mode of a Financial Institution.

  o Forum: Allows the member access to the Financial Institution on-line forum.

  - Schedule: Allows users to review scheduled on-line forums applicable to Financial Institutions.

  o FAQ's: A screen where Frequently Asked Questions and Answers to those questions are displayed, in this case particular to the operation of the Smarte System^{TM} from within the confines of a user in the mode of a Financial Institution.

  o Change Password: Allows the individual user to change their log-in password.

  o Demos: From this screen, the users can access demonstration portions of the system designed to give overviews of the system, in this case particular to the operation of the Smarte System^{TM} from within the confines of a user in the mode of a Financial Institution.

  o Downloads: From this screen, the users can download files that MoveMoney^{TM} have made available to "members" regarding the Smarte System^{TM}. Files may be technical briefs, FAQ files, Powerpoint (or other format), presentations, etc. In this case, downloads are particular to the operation of the Smarte System^{TM} from within the confines of a user in the mode of a Financial Institution.

  o Edit Profile: Allows the user to view, and perform limited edit to their profile.

  o Suspend My Activity: This screen permits the user, in case user suspects their accounts or access security has been compromised, to immediately stop all activity in the system related to themselves or accounts solely under their

68

control within the system. A Parent user stopping activity in this manner automatically ALSO freezes ALL CHILD entities and accounts as well.

o My Activities/Transactions: This screen allows the user to review their transactions and/or activity based on user settings such as date ranges and level of activity.

- Multiple Report Screens: Contains Reports applicable to Related portion of the system.

o User Administration: Allows a "super-user" at the Financial Institution to set-up additional users for their own institutions particular access.

- Selection/Mode: allows the Financial Institution to select existing users within their institution for profile and permissions edit.

  • Profiles: Add/Edit Screen for user profiles/permissions.

o Refer Merchant: This screen contains information similar to that where a merchant "signs up" on their own. This screen is provided for the Financial Institution to actively promote the Smarte System™ to individual merchants, thereby acting in the form of an Independent Sales Organization (ISO).

o Financial Administration: Allows the Financial Institution access to information regarding payments and/or commissions due from/to them in regards to MoveMoney.

- Multiple Report Screens: Contains Reports applicable to Related portion of the system.

o Buyer Maintenance: This is the primary entry screen for a Financial Institution to work with individual Buyers.

- Cancel Device: Redirects to Smarte Authentication™ Portion of System

- Issue New Device: Redirects to Smarte Authentication™ Portion of System

69

- **Activity Blocking:** Used to immediately suspend the activity of a Buyer and all child entities under that Buyer.

- **Forgot Password:** Used for the Financial Institution to retrieve a forgotten password of the Buyer. Note: This option requires the PHYSICAL presence of the buyer at the Financial Institution, as the issued physical security device is REQUIRED in order to access this information. This operation also sends a "log-in message" to the Buyer, suggesting that they change their password.

- **Manage Notifications:** Used to Manage Notifications based on activity to the individual Buyer.

- **Create New:** Primary Entry/Option Screen for the Financial Institution to enter a NEW buyer into the Smarte System^{TM}.

  - **Issue Device/Set Mode:** Redirects to Smarte Authentication^{TM} Portion of System.

  - **Add Accounts:** Used by the Financial Institution to enter/create new (sponsored) accounts for the Buyer.

- **Edit Profile:** Edit of a sponsored Buyer's profile information.

  - **Account Maintenance:** Edit of sponsored account information for the applicable buyer.

    o **Account Locking:** Stops the Buyer from utilizing this account, as well as locking the account from all "sub-buyers" under that individual Buyer. Also retains entry of REASON for the account being locked.

- **Sub-Buyer Maintenance:** Primary entry/option screen for the handling of "Sub-Buyers" under a sponsored Buyer.

70

- Create New: Primary Entry/Option Screen for the Financial Institution to enter a NEW SUB-BUYER into the Smarte System[TM].

  - o Issue Device/Set Mode: Redirects to Smarte Authentication[TM] Portion of System.

  - o Add Accounts: Used by the Financial Institution to enter/create new (sponsored) accounts for the Sub-Buyer.

  - Edit Profile: Edit of a sponsored Sub-Buyer's profile information.

- Activate Smarte Credit[TM]: Allows a Financial Institution to activate a sponsored Smarte Credit[TM] Account against an NSF ACH transaction.

- Pay Down Smarte Credit[TM]: A Financial Institution, sponsoring an activated Smarte Credit[TM] Account utilizes this screen to record payment receipt against the account from the individual Buyer.

- Manage Smarte Cash[TM]: Used to Create/Manage Smarte Cash[TM] accounts (sponsored by the individual Financial Institution) for a particular Buyer.

The main Screen layout for the Seller User is displayed in FIG. 15. The basic areas are as follows:

- Seller (Main): Primary entry/option screen for members functioning in the mode of a Seller.

  - o Forum: Allows the member access to the Financial Institution on-line forum.

    - Schedule: Allows users to review scheduled on-line forums applicable to Sellers.

71

o FAQ's: A screen where Frequently Asked Questions and Answers to those questions are displayed, in this case particular to the operation of the Smarte System™ from within the confines of a user in the mode of a Seller.

o Change Password: Allows the individual user to change their log-in password.

o Review Accounts: Displays Seller accounts and attachments to Product Classes, Balances, and any activity scheduled against the account(s).

o Demos: From this screen, the users can access demonstration portions of the system designed to give overviews of the system, in this case particular to the operation of the Smarte System™ from within the confines of a user in the mode of a Seller.

o Downloads: From this screen, the users can download files that MoveMoney™ have made available to "members" regarding the Smarte System™. Files may be technical briefs, FAQ files, Powerpoint (or other format), presentations, etc. In this case, downloads are particular to the operation of the Smarte System™ from within the confines of a user in the mode of a Seller.

o My Profile: Allows the user to view, and perform limited edit to their profile.

o View Critical Activity: This screen is used to view any critical activity log items that have not been "flagged" by the buyer as "read". Also permits buyer to "flag" critical activity items to "archive".

 ▪ Multiple Report Screens: Contains Reports applicable to Related portion of the system.

o Suspend My Activity: This screen permits the user, in case user suspects their accounts or access security has been compromised, to immediately stop all activity in the system related to themselves or user level accounts solely under their control within the system. A Parent user stopping activity in this manner automatically ALSO freezes ALL CHILD entities and accounts as well.

72

o My Activities/Transactions: This screen allows the user to review their transactions and/or activity based on user settings such as date ranges and level of activity.

■ Multiple Report Screens: Contains Reports applicable to Related portion of the system.

o Manage Blocks: Entry/Maintenance of Shipping restrictions within the system.

o Review Fees/Commissions: Displays set fees and commission structures set up for that particular Seller by MoveMoney.

■ Multiple Report Screens: Contains Reports applicable to Related portion of the system.

o Manage Returns: Displays and allows various status flags to be entered based on returns/failed transactions received/generated within the Smarte System^{TM}.

o Manage Inventory: Display Screen of basic platform/Interface options utilized by the Seller within the Smarte System^{TM}, as well as selection screen for Applicable Product Class to Review.

■ Product Class: Display of entries within the selected Product Class.

• Products: Allows add/edit/"delete" of Products, as well as attributes and graphic file designations for individual products under the selected Product Class.

• Tax Structure: Entry of Sales Tax Information by the seller for products/services under the particular product class.

The main Screen layout for the Buyer (Both Commercial and Retail Types) is displayed in FIG. 16. The basic areas are as follows:

- Buyer (Main): Primary entry/option screen for members functioning in the mode of a Buyer.

o Forum: Allows the member access to the Buyer on-line forum.

73

- **Schedule:** Allows users to review scheduled on-line forums applicable to Buyers.
  - o **FAQ's:** A screen where Frequently Asked Questions and Answers to those questions are displayed, in this case particular to the operation of the Smarte System™ from within the confines of a user in the mode of a Buyer.
  - o **Change Password:** Allows the individual user to change their log-in password.
  - o **Demos:** From this screen, the users can access demonstration portions of the system designed to give overviews of the system, in this case particular to the operation of the Smarte System™ from within the confines of a user in the mode of a Buyer.
  - o **Downloads:** From this screen, the users can download files that MoveMoney™ have made available to "members" regarding the Smarte System™. Files may be technical briefs, FAQ files, Powerpoint (or other format), presentations, etc. In this case, downloads are particular to the operation of the Smarte System™ from within the confines of a user in the mode of a Buyer.
  - o **Manage Notifications:** Used to Manage Notifications based on activity to the individual Buyer as permitted.
  - o **Shipping Address Selection:** This screen allows the Buyer to review/edit an existing shipping address, or initiate a new shipping address.
    - **Shipping Address Maintenance:** Buyer Shipping Address information add/edit.
  - o **My Activities/Transactions:** This screen allows the user to review their transactions and/or activity based on user settings such as date ranges and level of activity.
    - **Multiple Report Screens:** Contains Reports applicable to Related portion of the system.

74

o View Critical Activity: This screen is used to view any critical activity log items that have not been "flagged" by the buyer as "read". Also permits buyer to "flag" critical activity items to "archive".

- Multiple Report Screens: Contains Reports applicable to Related portion of the system.

- Suspend My Activity: This screen permits the user, in case user suspects their accounts or access security has been compromised, to immediately stop all activity in the system related to themselves or accounts solely under their control within the system. A Parent user stopping activity in this manner automatically ALSO freezes ALL CHILD entities and accounts as well.

o Shop: This is the primary entry/option screen for the Buyer in accessing the Smarte System™ Shopping "Mall".

- Search for Specific Merchant: Search Screen based on Seller Attributes, Product Categories Sold, or Name.
  - Product Info: Detail Product Information Screen.
    - o Add to Cart: Confirmation Screen of Item added to Buyer's Shopping Cart.
  - Merchant Info: Detail Seller/Merchant Information Screen.

- Search for Specific Product: Search Screen based on Product Keywords (Attributes), Categories, of Manufacturer Part/Item Numbers.
  - Product Info: Detail Product Information Screen.
    - o Add to Cart: Confirmation Screen of Item added to Buyer's Shopping Cart.
  - Merchant Info: Detail Seller/Merchant Information Screen.

- Order Screen: This screen serves to show the contents of the Buyer's shopping cart, as well as the status/cost of the order based on default shipping options. This screen also serves to give further options to the Buyer in order to confirm purchases.

    - Smarte Ad™s Checkout: Following a purchase, additional items are presented to the Buyer, based on "sub-products" identified within the system for those products/services purchased. The Buyer has the option of populating their shopping cart with any of the items presented, reverting back to the order screen.

    - Payment Options: Selection of payment methods and amounts from the available accounts for the Buyer.

    - Purchase Confirmation: This is the order confirmation screen, and initiates the order(s) to the seller(s), as well as all required transactions within the Smarte System™. May include secondary validation of "intent" to purchase by requiring device entry here.

    - Shipping Address Selection: This screen allows the Buyer to review/edit an existing shipping address, or initiate a new shipping address.

        o Shipping Address Maintenance: Buyer Shipping Address information add/edit.

- My Profile: Allows the user to view, and perform limited edit to their profile.

- Sub-Buyer Profile Maintenance Selection: Selection of Sub-Buyer to edit profile/information/limits for.

76

- Sub-Buyer Profile Maintenance: Sub-Buyer profile information (limited) edit.
  - Activity Blocking: Allows the Parent Buyer to "lock" activity for the selected Sub-Buyer.
  - Manage Access Blocks: Allows the Parent Buyer to create "blocks" against certain product categories.
  - Manage Accounts: Primary Entry/Option screen for the Parent Buyer to Select which accounts of theirs may be utilized by the Sub-Buyer, as well as provides for allocation of funds to use from those accounts.
    - Add Account: Allows Parent Buyer to Select and add and available account to the Sub-Buyer.
    - Edit Account: Allows Parent Buyer to allocate funds for use against the individual accounts existing for use by the Sub-Buyer.
    - Lock Account: Allows Parent Buyer to lock activity against an account, including the reason the account was locked.
- Account Management: Primary Entry/Option Screen for Buyer account management.
  - Review Accounts: Display Screen for all accounts in the system and balances/limits where applicable.
  - Pay Down Smarte Credit™: This option redirects the user to a display of the current Smarte Credit™ Balance(s) that are outstanding against their account(s). From here, the user selects the applicable account and payment amount.

77

- Increase Smarte Cash™: Allows Buyer to increase Smarte Cash™ account by taking funds from another account (with available amounts where applicable).
  - Send Smarte Cash™: Permits Buyer to transfer funds from their own Smarte Cash™ Account to another Independent Buyer's (NOT Sub-Buyer) Smarte Cash™ Account.

The main Screen layout for the MoveMoney™ Administration User is displayed in FIG. 17. Due to the complexity of the Administration User Screens, all of the screens are not displayed within FIG. 17. Additional Detail is displayed in FIG. 18, FIG. 19, FIG. 20, FIG. 21, and FIG. 22. The basic areas as displayed in FIG. 17 are as follows:

- Entry #2 – System Administration: First entry/option screen for MoveMoney™ Administrative users.
  - o Host Forum: Allows the user to Start/Take an on-line forum as a Host. This screen will also contain access to the Forum Schedule for all user modes.
  - o FAQ's: A screen where Frequently Asked Questions and Answers to those questions are displayed, in this case particular to the operation of the Smarte System™ from within the confines of a user in the mode of a System Administration.
  - o Change Password: Allows the individual user to change their log-in password.
  - o Security Officer Mode: This screen requests access to Security Officer Mode, displays Officer Activity Log, etc.. Also permits a Security Officer to Return to Standard Admin User mode if in Security Officer Mode.
  - o User (MoveMoney™) Admin (User Selection): This screen is the primary screen for selecting MoveMoney™ Administrative user profiles/security settings for Add/Edit/Delete.
    - Add User: Contains information entry and requirements for adding MoveMoney™ Administrative personnel.

78

(OR)

- Edit User: Contains information entry and requirements for adding MoveMoney™ Administrative personnel.

    - Permissions: Contains Permissions for applicable MoveMoney™ Administrative Personnel.

    - Security: Contains System Security Settings for applicable MoveMoney™ Administrative Personnel.

o Site Parameters: Primary Entry/Option Screen for Site Parameter Maintenance within the Smarte System™

    - Categories: Add/Edit/"delete" of Categories allowed for use within the system.

    - Account Codes: Add/Edit/"delete" of Account Codes allowed for use within the system.

o View Critical Activity: This screen is used to view any critical activity log items that have not been "flagged" by the user as "read". Also permits user to "flag" critical activity items to "archive".

    - Multiple Report Screens: Contains Reports applicable to Related portion of the system.

o Payment Processing: Primary Entity Selection Screen to record a payment against.

    - Payment Record: Entry of Payment record against an entity

o Smarte Cash™: Primary Entry/Option Screen for Smarte Cash™ Account Maintenance. Individual Account Selection Screen.

    - Manage Accounts: Allows Edit of Account Information, including increase based on direct receipt of funds from Buyer. Also permits locking of account based on status code change.

79

Express Mail No. EL179924489US

HOUSTON:64423/00030:655637v1

- **Balance Adjustments**: Direct Balance Adjustment to individual Account.
- **Multiple Report Screens**: Contains Reports applicable to Related portion of the system.

o Smarte Credit™: Primary Entry/Option Screen for Smarte Credit™ Account Maintenance. Individual Account Selection Screen.

- **Manage Accounts**: Allows Edit of Account Information, including increase based on direct receipt of funds from Buyer.
- **Balance Adjustments**: Direct Balance Adjustment to individual Account.
- **Multiple Report Screens**: Contains Reports applicable to Related portion of the system.

o Manage Smarte Devices™: Redirects to Smarte Authentication™ Portion

o Add FI: Refer to FIG. 18

o Manage FI: Refer to FIG. 18

o Add Seller: Refer to FIG. 19

o Manage Seller: Refer to FIG. 19

o Manage ISO's: Refer to FIG. 20

o Manage Buyer: Refer to FIG. 21

o Manage Transactions: Refer to FIG. 22

The Screen layout for the MoveMoney™ Administration User Financial Institution Management is displayed in FIG. 18. The basic areas are as follows:

- Manage FI: Profile Information edit Screen for Financial Institution already existing within the system.

- Add FI: Profile Information entry Screen for new Financial Institution being added to the system. Includes selection of applicable Financial Institution.

80

o Multiple Report Screens: Contains Reports applicable to Related portion of the system.

o Add Accounts: Account Information Entry Screen for new FI Accounts.

   ▪ Account Type Specific: Individual Screens containing information specific to the applicable TYPE of account being added or edited.

o Manage Accounts: Account Selection/Information Edit Screen for existing FI Accounts.

   ▪ Account Type Specific: Individual Screens containing information specific to the applicable TYPE of account being added or edited.

o Fees/Commissions: Fee and Commission detail Entry/Edit/"delete" Screen for applicable Financial Institution.

o User Admin: MoveMoney™ System Administration Access to User Information for selected Financial Institution. Primary User Selection Screen.

   ▪ Profiles: Selected User Profile/permissions information entry/edit.

o Manage Notifications: Adds/Edits/"deletes" Notifications for the individual selected Financial Institution based on events/conditions within the system.

The Screen layout for the MoveMoney™ Administration User Seller Management is displayed in FIG. 19. The basic areas are as follows:

- Add Seller: Profile Information entry Screen for new Seller being added to the system.

- Manage Seller: Profile Information edit Screen for Seller already existing within the system. Includes selection of applicable Seller.

o Multiple Report Screens: Contains Reports applicable to Related portion of the system.

o Shipping Blocks: Allows access to Seller's specified shipping area/location restrictions either at the Seller's specific level or as applicable to a single Product Class under the selected Seller.

81

o Product Class Maintenance: Add/Edit/"delete" detail entry/edit screens for Product Class(es) under the selected Seller.

o Tax Structure Selection: Access to Seller's specified Sales Tax Structure templates. This is the Selection Screen for individual templates.

- Tax Structure Edit: Access to Seller's specified Sales Tax Structure templates.

o Add Accounts: Account Information Entry Screen for new Seller Accounts.

- Account Type Specific: Individual Screens containing information specific to the applicable TYPE of account being added or edited.

o Manage Accounts: Account Selection/Information Edit Screen for existing Seller Accounts.

- Account Type Specific: Individual Screens containing information specific to the applicable TYPE of account being added or edited.

o Fees/Commissions: Fee and Commission detail Entry/Edit/"delete" Screen for applicable Seller.

o User Admin: MoveMoney™ System Administration Access to User Information for selected Seller. Primary User Selection Screen.

- Profiles: Selected User Profile/permissions information entry/edit.

o Manage Notifications: Adds/Edits/"deletes" Notifications for the individual selected Financial Institution based on events/conditions within the system.

The Screen layout for the MoveMoney™ Administration User Independent Sales Organization Management is displayed in FIG. 20. The basic areas are as follows:

- Manage ISO's: Primary Entry/Option Screen for Management of Independent Sales Organizations.

o Multiple Report Screens: Contains Reports applicable to Related portion of the system.

o Add ISO: Entry of NEW ISO to the System

82

- o Edit ISO: Edit screen for profile of existing ISO

- o ISO Attachments: Allows attachment of ISO's to one of more Sellers.

- o Fee/Commissions: Add/Edit/Delete of ISO Fee's and Commissions.

- o Accounts: Primary Add/Edit/Close option screen for ISO accounts.

    - Add Account: ISO Account profile ADD screen.

    - Edit Account: ISO Account profile EDIT screen.

    - Close Account: ISO Account profile EDIT screen. Includes REASON for closure of account.

The Screen layout for the MoveMoney™ Administration User Buyer Management is displayed in FIG. 21. The basic areas are as follows:

- Manage Buyer: Primary Entry/Selection Screen for Buyer Maintenance by MoveMoney™ Administration.

    - o Multiple Report Screens: Contains Reports applicable to Related portion of the system.

    - o Cancel Device: Redirects to Smarte Authentication™ portion of System

    - o Issue New Device: Redirects to Smarte Authentication™ portion of System

    - o Activity Blocking: Used to immediately suspend the activity of a Buyer and all child entities under that Buyer.

    - o Forgot Password: Similar to the screen used for the Financial Institution to retrieve a forgotten password of the Buyer. Note: Unlike the FI option that requires the PHYSICAL presence of the buyer at the Financial Institution, as the issued physical security device is REQUIRED in order to access this information, MoveMoney™ Administration does NOT require the Buyer to be present. This operation also sends a "log-in message" to the Buyer, suggesting that they change their password.

    - o Activate Smarte Credit™: Allows MoveMoney™ Administration to activate a sponsored Smarte Credit™ Account against an NSF ACH transaction.

83

o Manage Notifications: Used to Manage Notifications based on activity to the individual Buyer.

o Pay Down Smarte Credit™: A Financial Institution, sponsoring an activated Smarte Credit™ Account utilizes this screen to record payment receipt against the account from the individual Buyer. In this screen, MoveMoney™ Administration may enter payment received on behalf of the sponsoring FI, or enter directly if MoveMoney™ itself is the sponsoring FI for the account.

o Manage Smarte Cash™: MoveMoney™ Administrative Access to Smarte Cash™ accounts (sponsored by the individual Financial Institution) for a particular Buyer.

o Create New: Primary Entry/Option Screen for the Financial Institution to enter a NEW buyer into the Smarte System™.

  ▪ Issue Device/Set Mode: Redirects to Smarte Authentication™ portion of System

  ▪ Add Accounts: Used by MoveMoney™ Administration to enter/create new accounts for the Buyer. Allows specification of sponsoring FI.

o Edit Profile: Edit of a sponsored Buyer's profile information.

  ▪ Account Maintenance: Selection of existing account or option available to add an account.

    • Add Accounts: Used by the Financial Institution to edit Buyer accounts.

    • Account Locking: Stops the Buyer from utilizing this account, as well as locking the account from all "sub-buyers" under that individual Buyer. Also retains entry of REASON for the account being locked.

  ▪ Shipping Profiles: Access to Buyer Shipping Address information add/edit.

84

o Sub-Buyer Maintenance: Primary entry/option screen for the handling of "Sub-Buyers" under the selected "Parent" Buyer.

- Edit Profile: Edit of a Sub-Buyer's profile information.

  - Account Maintenance: Selection of existing account or option available to add an account.

  - Shipping Profiles: Access to Sub-Buyer Shipping Address information add/edit.

- Activity Blocking: Used to immediately suspend the activity of an individual Sub-Buyer.

- Create New: Profile Information Entry Screen for the MoveMoney™ Administration to enter a NEW Sub-Buyer into the Smarte System™ under the selected Buyer.

The Screen layout for the MoveMoney™ Administration Transaction Management is displayed in FIG. 22. The basic areas are as follows:

- Manage Transactions: The primary entry/option screen for the handling and maintenance of transactions within the Smarte System™.

  o Automated Check Handling (ACH): The primary entry/option screen for the handling and maintenance of ACH transactions within the Smarte System™.

  - Batch Processing: The primary entry/option/review screen for the handling and maintenance of ACH transaction Batches within the Smarte System™.

  - Return Processing: The primary entry/option/review screen for the handling and maintenance of ACH transaction RETURNS within the Smarte System™.

    - Process Return File: Selection and initial processing of Federal Reserve Bank Return File.

85

- Process NSF: Handling for ACH Transaction Returns due to insufficient Funds within the applicable account.
  - Resubmit/Cancel: Selection for Resubmission/Process
- Bad/Incorrect RTN/Account: Handling for ACH Transaction Returns due to Invalid or incorrect RTN/Account Combinations.
  - Information Correction/Resubmit: Allows edit of original transaction information and resubmission.
- R03 RTN Maintenance: Specific to R03 calculated RTN Financial Institutions and/or direct ACH only RTN's used in lieu of "published" RTN.
  - Formula Entry: Entry Screen for RTN related R03 formulas
- Process Buyer Rev/Denial of Auth: Handling for ACH Transaction Returns due to Buyer Revoking or Denying Authorization for the Transaction.
  - Auth Conf/Resubmit or Accept: Allows either confirmation of Buyer's claim (closure of Transaction) or denial of Buyer's claim and resubmission of transaction.
- Process Returns Unable to Match: Handling for ACH Transaction Returns received that can not be matched automatically due to either insufficient/incorrect return information within the Federal Return Transaction file, or return was misdirected.

86

- Process Closed Accounts: Handling for ACH Transaction Returns due to target Buyer Account closed externally to Smarte System™.

- Process Information Changes: Handling for ACH Transaction Returns due to Information Changes.

- Process Other: MANUAL Handling for ACH Transaction Returns not covered within standard options /areas of the Smarte System™.

- Multiple Report Screens: Contains Reports applicable to Related portion of the system.

  - Issue Credit Transaction: Selection of previously created/submitted ACH Transaction. Once selected, a reversing "credit" transaction can be created.

    o Smarte Credit™: The primary entry/option/review screen for the handling and maintenance of Smarte Credit™ Accounts within the Smarte System™.

    o Smarte Cash™: The primary entry/option/review screen for the handling and maintenance of Smarte Cash™ Accounts within the Smarte System™.

    o Multiple Report Screens: Contains Reports applicable to Related portion of the system.

The Screens for the Interface to the Smarte Authentication™ portion of the system are displayed in FIG. 23, FIG. 24, and FIG 25. The listing of these screens is as follows:

EUS01	Place Smarte CD™ in Drive
EUS02	Place Smart Card in Reader
EUS03	Specify Type of Device
EUS05	Access NOT Granted- customer service info
EUAS02	Data Entry and Activation Request
EUAS03	Approval, Source Link, Demo/Help Link

87

	EUAS04	NOT Activated- Customer Service Info
	EUAS05	Already Activated
	EUPW01	UNIVERSAL PASSWORD HOME
	EUPW02	UNIVERSAL PASSWORD ENTRY
5	EUPW03	UNIVERSAL PASSWORD CHANGE
	EUSO10	Kill Device/Authorization
	SAAUM01	Add End User/ End User Maintenance
	SAASU01	End User Selection
	SAAUT05	AUTHORIZATIONS TO BE GRANTED
10	SAESD01	Granted Device Control Authority Selection
	SAESD02	Granted Device Control Authority Detail
	SAESM01	External Source Profile
	SAESU01	External Source System User Selection
	SAESU02	External Source System User Profile
15	SAESU03	External Source System User Device ISSUE Capability
	SAESU04	External Source Super User Device Capability
	SAESU05	External Source Super User Device Issue Authorization - New
	SAESU06	External Source System User Device Issue Authorization - New
	SAIMP20	Import Device Info to Stock" and "Import Authorized User Information
20	SAINV01	Inventory Maintenance – Selection
	SAINV02	Device Detail (DISPLAY SCREEN ONLY)
	SAINV02A	Device Detail
	SAINV03	Device Access Authorizations
	SAINV04	Device Access Authorization Detail
25	SAINV05	Kill Device
	SAINV05A	Kill Device Access Authorizations
	SAINV06	External Source Selection

88

	SAINV09	Device Access Authorization Master
	SAINV09W	Authorization Master WARNING
	SAINV32	Master Device List
	SAINV40	Authorization Master List
5	SAINV41	Interface Information Request
	SAINV42	External Source System User Home Page
	SAINV43	Removing External Source
	SAINV44	End User Authorization Master
	SAINV45	External Source Device Listing
10	SAINV47	END USER Devices
	SAINV47A	END USER Devices
	SAINV48	Device Detail Entry
	SADEVxxx	DEVICE READ SCREENS (MULTIPLES)
	SAINV49	Activation Entry
15	SAINV50	Device Selection/Issue to External Source
	SAINV51	Device Lot Issue to External Source
	SAINV52	Device Lot Transfer
	SAINV53	Device Lot Transfer
	SAINV54	Device S/N Range Issue to External Source
20	SAINV55	Device S/N Range Transfer
	SAINV56	Device S/N Range Transfer
	SAINV57	Selected Device Issue to External Source
	SAINV58	Selected Device Transfer
	SAINV59	Selected Device Transfer
25	SAMAA01	Mass Auth Assignment

SYSTEM DATA STRUCTURE

89

The methodology used in defining the structure of the system is one where any "thing" that either has, or could have multiple "types", is structured so that there is a "master" table, containing information that would be common to ALL types, as well as an identifier code within this record indicating the specific "type". Related to this "master" data table, are individual tables

5   then that contain information specific to the individual "types". When a new "type" is added, while additional code will have to be created within the system itself to handle this new "type", the "master" table does not have to be altered, and the addition of a specific type table is all that is then required. Based on this principle, there is no need to have to "redesign/restructure" the system in order to add a new entity type. This methodology has significant advantages in that

10   additions to the system can be "plugged in" rather than having to redesign/recode entire sections of the system or adding additional fields to data tables that would only be used for that specific type. The Smarte System™ Data Table Structure and inter-table relationships (one to many, many to one, one to one) is depicted in FIG. 26. The descriptions of the items in FIG. 26 are detailed in the Table in FIG 27.

15   DEVICES

Access to the system is granted to End Users via a Device. Devices are initially maintained by the system in an "inventory", and are grouped sequentially by "Lots". This relationship is displayed in FIG. 9. Physical Devices are supplemental to the individual user's Standard Login and Password. Once the Login (and Password/Supplemental Information) is/are

20   received by the MoveMoney™ Security Server, the information is then matched to the System's Database. The Type of device that the user has been issued is then retrieved by the system. Dependant upon the type of issued device, the system then requests additional information from the user, by either direct data entry or physical device insertion into the appropriate reader. From this, the information obtained is then validated via the security system, whether it can be

25   processed internally, or passed to an outside agent, (such as the RSA ACE Server) with MoveMoney's Security System acting as the intermediary between the systems. This methodology allows the MoveMoney™ Smarte Authentication™ System to maintain a map

90

between multiple systems and device types, as well as provide the future capability to allow cross platform access between participating entities.

The Smarte Authentication™ portion of the system is designed to allow virtually any device "type" to be utilized for authentication purposes. The device types currently employed/structured for in the system are: Smarte CD™; Smart Card; Soft ID; and 3rd Party Tokens.

The Smarte CD™ is a serialized device application of a standard business card sized CD ROM disk, playable in virtually any existing data type capable CD Drive. A picture of the Smarte CD™ is shown in FIG. 28 and FIG. 29.The Smarte CD™ has the following "optional" features, of which one or both types of "serialization" must be incorporated in order for the CD itself to be a viable means of authentication of the individual user:

- Serialized "Content" File (Style I): This file is a 220 character "intelligent" encrypted file that allows the individual CD to be tracked not only be Serial Number, but date of generation and individual generation site. Encryption follows MoveMoney™'s proprietary Random Based encryption methods, and is decipherable only by the MoveMoney™ CD Generator unit. Because the Decryption code does NOT reside anywhere on the Server, but within Stand-alone units NOT tied directly to access from the Internet, it is safe from remote access/hacking. Refer to Chapter 2 for limitations regarding Serial Number Generation.

- Source Serialized Content File (Style II): This is simply a file that is written to the CD, based on a file list of Serial Numbers generated externally to the MoveMoney™ system. There is no encryption given for this. Some of the advantages to this type of file is that the serial numbers themselves can be generated and read by External sources/customers, and the actual size/contents of this file is solely up to the customer themselves, although the file name MUST

91

remain consistent, UNLESS the CD is NOT to be used with the MoveMoney™ Smarte Authentication™ System, but an external entity authentication system.

- Source Serialized Content Retention: This is information retained by the MoveMoney™ system that is mapped/linked to the Serialized Label ID/Content file, based on a file list of Serial Numbers generated externally to the MoveMoney™ system. Some of the advantages to this type of file is that the serial numbers themselves can be generated and read by External sources/customers, and the actual size/contents of this file is solely up to the customer themselves, without impacting the CD file generation parameters. In this case, the MoveMoney™ 220 Character Serial Number Content File is STILL written to the CD for validation/tracking.

- Serialized CD Volume Label: The Volume ID label of the CD itself can be serialized, however the inherent limitation to this is the limited number of characters that can be applied to the Standard Volume Label ID. Note that while Volume ID Serialization can be done ALONE (without MoveMoney™ Serial Number Content File), without the Content file, the CD cannot be utilized with the Smarte Authentication™ program.

- Standard Copy Protection – Prevents most CD Burner copy software from outright duplication of the MoveMoney™ CD, however does not prevent "re-mastering" of the contents of the CD. Utilizes a technique that defects a portion of a known file to create a specific error that cannot be easily duplicated by common duplication hardware or software.

- Smarte Authentication™ Original CD validation [Available ONLY via Smarte Authentication™ System/MoveMoney's Plug-in interface or Smarte system]. Ability to validate whether or not the CD is an original MoveMoney™ generated CD or a copy.

92

-   Additional Content can be added at the end users requirement. Serialized CD's can be produced from "blanks" and a single "master" content CD supplied by the end user.

The Smart Card is a serialized device application of a standard Smart Card in use today. The Smarte ID™ Smart Card as produced by MoveMoney, an example of which is displayed in FIG 30, is about the size and shape of a standard business or credit card for each of portability. These cards initially , when issued to the External Sources, will contain NO information. Since ALL Smart Card Readers are ALSO Writers, MoveMoney™ has the ability to provide anti-piracy techniques through the use of "secure" Smart Cards, requiring the use of a "password" send to the card in order for the information to be read or altered. If the card can be successfully written to using the proper password, the card is likely an original and not a "forgery". Since the system can also detect the Type of card, and the type of card requires the password, it becomes virtually immune to successful forgery. The functionality/cross application utilization of the Smart Cards are limited by the current lack of industry standards regarding the embedded chips themselves, so MoveMoney™ and External Sources need to set up a "Smart Card Cross Reference" usability chart for External Sources to refer to as the varying Smart Cards are incorporated into the system. In addition, due to the current lack of "standards" regarding the Smart Cards themselves, the "type" of Smart Card itself must be maintained within the system, as programming/API calls/etc will vary from one individual card type to another.

The Soft ID is a program, file, or combination of these that reside on a particular machine, and allow the system to identify the individual, as being allowed to access from either a single or multiple machines. Typically, these forms of identification are no as strong inherently as a physical authentication device, as they are relegated to the machine, and are as accessible for identity theft as the Soft ID is able to be copied or moved from the individual machine, or access to the individual machine is gained by an individual having the real user's password. Despite these factors, they are used, so the Smarte System™ is structured/designed to allow for their usage.

93

The 3rd Party Device type is any device, system, or combination of such that functions in a manner to physically authenticate a user's identity. Devices, such as RSA's SecurID™, rely not only on the device itself, but on proprietary system's from which the validation occurs. In order to utilize such devices and system's within the Smarte Authentication™ System, the system is designed to interact with external systems via these external system's "plug-ins" or equivalent interfaces. In this manner, a user can utilize the physical device of a third party, without having to purchase or maintain the operating system behind it, utilizing the Smarte Authentication™ System as the portal for validation instead. An example of such a device (RSA's SecurID™) is shown in FIG. 30.

SYSTEM FLOW

There must be a mechanism to access and interface with the individual Seller's systems in order to provide the Buyer Interface between the Seller's System and the Smarte System™. There are various models and methodologies regarding the manner in which this interface is accomplished. Rather than create a series of scripts that are added to the Seller's system in order to interface with the multitude of individual "check-out" programs, both third party and "custom", it was determined that a better way to accomplish this was to DIRECTLY interface with the Seller's system itself. In addition to this unique platform, a secondary version of the platform that was designed solely to facilitate the payment itself, without any of the other capabilities. This, in effect, gives the Seller's additional options on how they want to set-up and interact with the MoveMoney™ System.

The Smarte VII™ platform is an external program that resides on the individual Seller's Server, interfacing with the MoveMoney™ Smarte System™. It contains the required interface to the individual Seller's system, a complete electronic "shopping cart", as well as other standard features incorporated in the Smarte System™ itself for use by Sellers utilizing the Smarte System™ inventory directly. Those features that are common to the Smarte System™ itself are:

-   Full Function Unified E-Shopping Cart
    o   Order Verification/Summary Screen

94

o   Seller QOH Verification

-   Seller System Update (updates in either Seller's or Smarte System^{TM} as applicable)

-   Smarte Ads^{TM}

5   The Smarte VII^{TM} Platform is based on a series of platform independent applications that are custom configured at Seller sites. The Platform provides MoveMoney^{TM} a dynamic link to the Seller database system. The Platform also provides for dynamic validation of the Seller (Smarte Certify^{TM}) through the Private/Public key pair rings and the Digital Signatures programmed through the application. The Smarte VII^{TM} infrastructure provides a common

10 ground and the base structure needed for current applications as well as future product offerings. The Smarte VII^{TM} architecture also ensures Security by linking the Buyers and Sellers to the MoveMoney^{TM} system, keeping track of the multiple sessions that are opened and closed during the checkout process. The design allows for automatic encoding of all data using special hashing routines, and encrypting of the same data for security against spoofing. Incorporating these

15 features within the Smarte VII^{TM} System itself provides the following benefits:

-   The MoveMoney^{TM} Server is not burdened with the processing requirements for these segments.

-   Security is increased, as there is less electronic "traffic" of information between the Servers.

20 -   Increased Performance.

In addition to these features, the connection between the Seller's Server and the MoveMoney^{TM} Serve is "invisible" to the Buyer. Since all Sites have the same "look and feel" to them, whether the Smarte VII^{TM} system or the "check-out/purchase" system within the Smarte System^{TM} itself, it provides a "universal" feel to the Buyers utilizing the system. As part of the

25 interface, the Smarte VII^{TM} system provides the ability to verify inventory quantity on hand (available stock), providing that all the requirement are met. In addition, as part of the interface to the Seller's System, the Smarte VII^{TM} System has the capability to directly interface with the

95

Seller's Order Entry System, and does so provided certain conditions have also been met. The basic Flow of the Smarte VII^{TM} system is illustrated in FIG. 32, which shows the process whereby the user enters the system from the "Smart Purchase" icon on the Seller's Web Page itself. The system is activated from the Seller's Web page through a graphic "banner" on the page that links directly to the Smarte VII^{TM} System. The placement of this activation banner is NOT within the standard Checkout portion of the Seller's site, but next to the link that the Seller's site provides to enter the Standard Check-out System. Once the Buyer selects the option to purchase items from the Seller the "Smarte" way, the Seller's Authentication Certificate is presented to the Buyer. This shows the Seller to be legitimate, and establishes a "secure" connection between the Buyer's internet browser and the Seller's Server. The Seller is then Presented with the Smarte System^{TM}'s Electronic Shopping Cart. This allows the Buyer to select from inventory/services listed/maintained by the Seller. This is a full function electronic shopping cart.

Once the Buyer has selected the desired product(s)/service(s), they select the option to "Buy". Once this option is selected, the Buyer is presented with the User Log-In Screen [8]. The User is required to enter Log-In Name and Password. Once this is accomplished and the Buyer selects to continue, the following occurs:

- A connection between the Seller's Server and the MoveMoney^{TM} Server is established (secure connection). This connection remains open to the point where the ORDER Information is transmitted back to the MoveMoney^{TM} Server (Smarte System^{TM}), OR the Buyer terminates the session.

- The Buyer's Login Name and password is encrypted and sent to the Smarte System^{TM} (MoveMoney^{TM} Server). This information is used by the Smarte System^{TM} to identify the individual Buyer and retrieve the applicable information required by the Smarte VII^{TM} System to process the order.

The information transmitted from the Smarte System^{TM} to the Smarte VII^{TM} system is as follows:

- Buyer Validation information (Credential Information only: Buyer Login/Password validated on the MoveMoney™ Server).

- Buyer Account information and Available amounts (Account Detail Names transfer only, NOT the identifying information for the account itself.

5
- Buyer Shipping Address Information (detail).

- Buyer Preferences for Shipping Methods

- Seller Limitations (if any) placed on Methods of Shipment, Locations, and Payment Options.

The data is transferred via an encrypted EDI format. This is done, as the number of
10 records transmitted back, with the exception of the Validation information, will vary. Once the Smarte System™ has received the required information, the Buyer is requested to authenticate their identity with the physical credential issued to them by the original sponsoring Financial Institution. The information obtained by the Smarte VII™ System is verified against the information obtained from the Smarte System™. Once the Buyer's identify has been
15 authenticated, the Smarte VII™ System performs Tax and Shipping Calculations based on the following:

- Items/Services Purchased

- Sales Tax from Seller's Specified Tax Structure

- Shipping Charges based on Buyer's preference and default Shipping Address

20
- Charges, if any, from default payment account(s)

If any of the original Defaults are outside of the limitations placed by the Seller, or there is insufficient funds available in the Buyer's default account to process the order, then the Buyer is presented with a "Sales Warning" information window, listing any items in conflict. Warnings issued to be as follows:

25
- The <Default/Selected/Entered> Shipping Address you have <Selected/Entered> is outside of <the Seller's Name>'s specified <Shipping/Service> Area. This

97

message is followed by Seller's specific Shipping/Service Location Restriction Information

- The <Default/Selected/Entered> Telephone Area Code for the Shipping Address you have <Selected/Entered> is outside of <the Seller's Name>'s specified <Shipping/Service> Area. This message is followed by Seller's specific Shipping/Service Telephone Code Area Location Restriction Information

- The <Default/Selected/Entered> has restrictions on the Telephone Area Code Locations <Serviced/Shipped to>. You have not entered a Telephone Area Code for the Address you have <Selected/Entered>. This message is followed by Seller's specific Shipping/Service Telephone Code Area Location Restriction Information

- Your Purchase does not meet <the Seller's Name>'s Minimum Purchase Quantity for the following Item<s>: Followed by List of items with variances

- The Total Amount of you order does not meet <the Seller's Name>'s Minimum Purchase Amount Requirement of <Minimum Purchase Amount Total Required by Seller>. Buyer given option to return to Shopping Cart to Adjust Order

[OR]

Buyer given option to Purchase anyway, paying the minimum Purchase amount for the order as is in order to meet the minimum requirement.

- The following Account<s> you have selected do not have sufficient available funds to Process this Order:
  o List of Accounts with variances
  o Follow this with the following: This may be due to temporary reserve holds placed on available funds in the listed account<s>.

Additional Warnings may apply and be added to the system as they are needed. The Buyer is then presented with an order summary screen that lists the following information:

- Buyer's Name

98

- # of items/services purchased
- Ship to Address
- Method of Shipment
- Payment Options
- Tax and Shipping Charges
- Total Amount of order

The Payment Options are referred to ONLY by the Buyer's descriptive name for them. The actual account detail identifications are NOT transmitted to the Smarte VII^{TM} system. In addition to the detail listed above, the screen will also note delayed payment options as applicable to selected payment methods, dictated by the Seller. Any items in conflict are also noted on this screen. ONCE THE BUYER HAS REACHED THIS POINT IN THE PROCESS, ANY ATTEMPT TO USED THE "BACK" BUTTON ON THE BROWSER FORCES THE BUYER TO RE-LOGIN/VALIDATE IDENTITY. From this screen, the Buyer can then select to Change the following, for which a separate window/screen appears for each one.:

- Ship to Address (with option to add/update this change in the Smarte System^{TM} automatically)
- Method of Shipment
- Payment Options

As the Buyer makes any changes to any of this information, the Total for the order is calculated dynamically in order for the Buyer to easily determine the effects on the price of the order. Once the order is acceptable to the Buyer, they then select "OK" to complete the order. Note that the Buyer is prevented from completing the order if any conflicts exist. If any conflicts exist, the Buyer is redirected to the "warning" screen. Once the order is acceptable to process, Quantity on Hand and Seller System Updates, as applicable, occur. Note that any interface to the Seller's System that occurs, as with the selection of the inventory items presented in the electronic shopping cart, is a custom interface tailored to suit the needs of the individual Sellers.

99

Quantity on hand (available stock), may be verified/relayed to the Buyer providing that ALL of the following conditions are met:

Seller's applicable database must be available to the Smarte VII™ System. If the Seller's System utilizes an alternate Check-out system, this System MUST update quantity on hand within the inventory system OR directly input into the Order Entry portion of the Seller's system. Seller must NOT be a "true" e-commerce business, whereby the Seller does not maintain an internal inventory. Seller must PERMIT the Smarte System™ to notify the Buyer of a potential NIS condition. In regards to the Smarte VII™ System's capability to directly interface with the Seller's Order Entry System, the Seller must permit the interface. Factors, which may prevent the Seller from permitting this, are as follows:

- The Seller has only limited access to the Order Entry Portion of the individual program used.

- The Seller is prevented by software provider Legal or Maintenance Agreement(s) from direct input of data into the system.

At this point, the Smarte VII™ system Generates the order record information for transmission. As with the transmission of information from the MoveMoney™ Server (Smarte System™) to the Seller's Server (Smarte VII™) is accomplished utilizing an encrypted EDI block, so too is the transmission of the ORDER information itself transmitted back to the Smarte System™ from the Smarte VII™ System. As with the initial transfer of information, the number of actual records may vary. Once this transmission occurs, the connection between the MoveMoney™ Server and the Seller's Server is terminated. The Buyer is then presented with the Smarte Ads™ Screen, which lists additional products that may be of interest to the Buyer based on the purchase just accomplished. This Information is driven from the listing of additional products that the Seller has chosen to add to the Smarte System™ Data Structure. The format for the transmission of return data initially from the MoveMoney™ Server (Smarte System™) to the Seller's Server (Smarte VII™) is as follows:

- Header Record

100

- o Buyer Base Required Profile Information
- o Buyer Accounts
- o Buyer Addresses
- o Buyer Preferences of Shipping Methods
- o Seller Location Limitations
- o Seller Shipment Method Limitations
- o Seller Payment Method Restrictions
- Trailer Record

The format for the transmission of Order data from the Seller's Server (Smarte VII™) to the MoveMoney™ Server (Smarte System™) is as follows:

- Header Record
  - o Seller Identity
  - o Buyer Identity (MMCIDENT)
  - o Order Primary information
  - o Accounts Used/Amounts
  - o Line Items in Order
  - o Shipping Address Selected
  - o Shipping Address Alteration (includes "update/add to profile" option for Buyer)
- Trailer Record

The Buyer Login and validation process may alter based on Security Requirements and type of Credentials used. For example, if a "Smart Card" is used, another connection to a third (external) server may be required in order to validate the information entered. This will be determined based on changes, if any, to the security requirements in the future.

The Smarte VII™ Light "Plug-in" is designed to facilitate an even quicker interface with multiple merchants' sites. This also provides an alternative for those merchants who are unwilling to accept our full platform on their site, or to interface in any way with their own

101

internal systems. The basis for this design, similar to the Smarte VII™ full platform, is that a form is created which resides on the Seller's server. This form acts as a "gateway" to the MoveMoney™ Server and subsequently Smarte System™. This form is used solely to collect and pass the required information to the MoveMoney™ Server from the Seller, along with the

5   login and password from the Buyer. From there, only a confirmation of payment number (the MoveMoney™ Order Identification# that is assigned within the Smarte System™) is returned to the seller. The end result of the process is that the Seller's system receives an Authorization from the Smarte System™ instead of the normal credit card authorization, and instead of payment type as "Visa", "M/C", "AMEX", it becomes "MoveMoney™". Since the basis of this plug-in is

10   strictly to provide a means of payment, the following apply:

-       There is no physical identification (Smarte Device™ verification)

-       There is no check-out or interaction with Sellers Databases

-       There is no option for Buyer to Select Accounts, and therefore no split payment as well.

15   NOTE: THIS IS CONSIDERED A HIGH RISK TYPE TRANSACTION BY MoveMoney™ ON BEHALF OF THE SELLER. The flow of the Smarte VII™ Light system is as shown in FIG. 32.

An alternative to Smarte VII™ and Smarte VII™ Light Incorporation specified here is where the functionality of the Smarte VII™ and Smarte VII™ Light systems resides on the

20   MoveMoney™ Server. This functionality has been incorporated for situations where the Security of the Individual Seller's site may be in question. In cases such as this, the Smarte VII™ and Smarte VII™ light functionality is performed from the MoveMoney™ Server instead of the Sellers. In this scenario, information processing is handled internally within the MoveMoney™ Server, and only the confirmation and final confirmed order information, as applicable, is

25   transmitted back to the Seller's Server. The drawback to this option is the increased processing on the part of the MoveMoney™ Server itself, however this can be overcome as needed with upgrades/additions to existing hardware if the need arises.

102

The Smarte Authentication™ System Plugin can be segregated into two basic functional classifications as User Authentication and Product (CD Based Media Distribution).

User Authentication is utilized as a third layer of access security to help positively identify the user, and to validate that the user is in fact, not another individual posing as that user. There are 4 requirements within the system, regardless of application or utilization logistics that are required in order for the device/auth/system to function:

1. Device must be physically in the hands of the end user.

2. Device must be attached/assigned to the individual end user in the SA system.

3. Access Authorization must be attached to the device.

4. Device must be activated (End user identity verification - entered into the system)

One of the requirements for the User Authentication to be effective rests with the external user, and the design/set-up of their system. If the Authentication is to act as a prevention of unauthorized access, then the external source system MUST prevent users from being able to "bookmark" and enter areas of the system directly, that are "behind" the access/login screen. User Authorization falls into two separate categories. This is done to highlight the varying complexities required to be maintained between the capabilities of the two systems. Option I is the simple form of the usage of the system. Under this category, each user maintains only a SINGLE device, of a single FIXED type utilized by the external user. An example of this would be a business, whereby they have chosen to utilize ONLY Smart Cards within their organization. Each user within this organization can only gain access through THAT particular Smart Card, and each user is only issued a SINGLE card. Note that this option is anticipated to be more common for organizations utilizing the system to validate user access for internal systems, rather than those systems that are exposed to the general public. This feature does not prevent the user from maintaining MULTIPLE devices, it simply limits the access to the particular external source. This Plugin option functions independently of the User's maintained devices, however, this option, when elected by the source, prevents the "mapping" functionality of the Smarte Authentication™ system. The basic flow within a system utilizing Option I (refer to FIG. 34) is

103

as follows: When a user accesses a site that has the Option I Type Smarte Authentication[TM] Plugin incorporated, the site passes the user's login and password information to the Smarte Authentication[TM] Plugin. The Plugin establishes a link to the MoveMoney[TM] Security server, and passes the user's password and login, the source id, and device information to the Security

5   Server for validation. All of this information is possible in one pass, as there is only a single device type, the requirement for information/device read is already known, and can therefore be requested/obtained AT the time of login. If Physical Device validation is required, it is also performed prior to the transmission of information. Once the MoveMoney[TM] Security Server receives this information, it validates against the information stored on the server within the

10   user's profile. Regardless of results, information is then transmitted from the Security Server to the Plugin, which then takes appropriate action in redirecting the user to a new address depending upon the results returned, based on the settings previously stored by the external source administrator. If the validation of the information passed requires that an external security server or program be accessed, it is done so from the MoveMoney[TM] Security Server, and NOT

15   by the Plugin independently. Option II is the more complex model, and takes into account the ability of an external system to recognize multiple device types, as well as the fact that the user themselves may maintain more than one device with which to access the system. The flow for Option II is as shown in FIG. 35.The initial requirements and resultant action for Option II is the same as with Option I except for the additional complexity requirements. At the point of User

20   Login, there is NO device interaction, as the TYPE of device is NOT known. Therefore, only the Plugin Source Identification, and entered Login/password are transmitted to the MoveMoney[TM] Security Server. Once the user is identified via the source and Login information, and password is validated, device information is then transmitted back to the Plug-in for ALL available types of devices. IF the user has multiple devices available to them for the identified SOURCE, then a

25   screen is presented to the user to select device type to use. Once the type of device to use has been identified, validation of the device is then performed, with the condition that if the device validation is not a fixed type, OR requires an external server/system in order to validate the data,

104

the information must then be transmitted BACK to the MoveMoney™ Security Sever to handle the additional validation step. If this occurs, the results of the validation are then passed back to the Plugin. If additional transmission/validation is not required, then the Plugin itself can validate the information from that previously transmitted based on the device type. In addition to the

5   Option I and Option II application methodologies, there are additional methodologies that can be employed by the External Source depending upon their individual requirements. These basic application variant scenarios are displayed in FIG 36 and Fig 37. These variations to the application of the Smarte Authentication™ take into account whether the External Source has required ALL of their users to utilize a device, or only a partial number of them, (such as in an

10 initial pilot or test program), whether they have decided to allow the use of "universal passwords" as an option, or even if they have chosen to have the Smarte Authentication™ system handle ALL of the access requirements, including the maintenance of their user base and subsequent handling of periodic or access fees via the Smarte System™ Fees and Commissions capability.

15   The Plugin, regardless of the application, passes information between the Smarte Authentication™ portion of the system and the External Source Page, as well as collect information from the End User. The Plugin acts as the information "hub" of the Smarte Authentication™ portion of the Smarte System™. Information Requirements are depicted in FIG. 38. For the purposes of clarity, within FIG. 38 and within the following listing, the term

20 "SA Prime" refers to the Smarte Authentication™ System portion of the Smarte System™ residing on the MoveMoney™ Server and not the Smarte Authentication™ Plugin. Information passed in the various segments depicted in FIG. 38 is as follows:

Passed Information Requirements: Source to Plugin

Source Adds End User to System

25   -   External Source SA System ID

        -       End User Login Name (or other Unique Identifier for the End User for that particular External Source

105

- Personal Identifier Information #1 (Optional – Use depends on Source Activation Requirements)
- Personal Identifier Information #2 (Optional – Use depends on Source Activation Requirements)
- Existing SA System ID for User (if exists/known)
- Personal Information (Optional)
  o Name Prefix
  o First Name
  o Middle Initial
  o Last Name
  o Name Suffix
  o Address Line #1
  o Address Line #2
  o City
  o State
  o Zip Code (5)
  o Zip Code (4)
  o Voice Telephone #1
  o Voice Telephone Ext (#1)
  o Voice Telephone #2
  o Voice Telephone Ext (#2)
  o Email Address
  o SSI#

Authorization Request

- External Source SA System ID
- End User Login Name (or other Unique Identifier for the End User for that particular External Source that was previously passed to the SA system

106

- SA System ID for applied Access Authorization
- "0" if Single Device/One Device for user Known (External Source Sets up as an internal requirement); or "1" if "standard" utilization
- "2" if Password passed to system", "3" if not
- "4" if Dynamic URL passed, "5" if not
- "6" if Dynamic Strings Passed, "7" if not
- Connection/Session ID/Request Number
- If Single Device Type known:
  o Code indicating expected type of device
- Password Passed (Optional usage/utilization depending on Universal Password Override/Usage)
- If Plugin WILL handle Redirection utilizing Dynamic variables, the following information is required [Note: This information is retained by the Plugin and not passed to the SA Prime]:
  o If Dynamic URL:
     - URL to Redirect to if good
     - URL to Redirect to if bad
     - URL to Redirect to If Not Found
  o If Dynamic Strings to be passed
     - String to Pass if good
     - String to Pass if bad
     - String to Pass If Not Found

Passed Information Requirements: Plugin to SA Prime

Source Add End User Information

- External Source SA System ID
- End User Login Name (or other Unique Identifier for the End User for that particular External Source

107

- Personal Identifier Information #1 (Optional – Use depends on Source Activation Requirements)
- Personal Identifier Information #2 (Optional – Use depends on Source Activation Requirements)
- Existing SA System ID for User (if exists/known)
- Hash Value
- Personal Information (Optional)
  o Name Prefix
  o First Name
  o Middle Initial
  o Last Name
  o Name Suffix
  o Address Line #1
  o Address Line #2
  o City
  o State
  o Zip Code (5)
  o Zip Code (4)
  o Voice Telephone #1
  o Voice Telephone Ext (#1)
  o Voice Telephone #2
  o Voice Telephone Ext (#2)
  o Email Address
  o SSI#

Device Information
- External Source SA System ID
- Connection/Session ID/Request Number

108

-   End User Login Name (or other Unique Identifier for the End User for that particular External Source

-   Code indicating type of device

-   Serial Number of Device (Encrypted String as Read from Device)

-   Anti-Piracy Result Code: "0" – Pirate Copy Determined; "1" Valid Device; "2" – Not Determined

-   SA System ID of Device

-   IP of User (if captured)

-   Hash Value

Authorization Request

*   [Note: Dynamic Strings are retained by the Plugin, but are still passed to the

SA Prime for Log retention]

-   External Source SA System ID

-   End User Login Name (or other Unique Identifier for the End User for that particular External Source that was previously passed to the SA system

-   SA System ID for applied Access Authorization

-   "0" if Single Device/One Device for user Known (External Source Sets up as an internal requirement); or "1" if "standard" utilization

-   "2" if Password passed to system", "3" if not

-   "4" if Dynamic URL passed, "5" if not

-   "6" if Dynamic Strings Passed, "7" if not

-   Connection/Session ID/Request Number

-   Hash Value

-   If Single Device Type known:
    o   Code indicating expected type of device
    o   Device Serial Number (String)

109

o Anti-Piracy Result Code: "0" – Pirate Copy Determined; "1" Valid Device

- Password Passed (Optional usage/utilization depending on Universal Password Override/Usage)

- If Plugin WILL handle Redirection utilizing Dynamic variables, the following information is required [Note: This information is retained by the Plugin and not passed to the SA Prime]:

   o If Dynamic URL:

      ▪ URL to Redirect to if good

      ▪ URL to Redirect to if bad

      ▪ URL to Redirect to If Not Found

   o If Dynamic Strings to be passed

      ▪ String to Pass if good

      ▪ String to Pass if bad

      ▪ String to Pass If Not Found

Passed Information Requirements: SA Prime to Plugin

Device Types Available

- External Source SA System ID

- Connection/Session ID/Request Number

- End User Login Name (or other Unique Identifier for the End User for that particular External Source

- Code Block indicating type of device

(Examples: for a CD only: "0" for a CD and MoveMoney™ Smart Card: "02"; for a CD; MoveMoney™ Smart Card; and Secure Concepts Token: "025"; for Two (2) CD's and Two (2) MoveMoney™ Smart Cards with One (1) RSA token: "00224"

110

- Code Block indicating SA System ID's for specific Devices Available – Listed in same order as in Code Block for type of device
- Indication of whether Anti-piracy Techniques to be utilized by the Plugin
- Hash Value

Authorization Request [Results]

* [Note: Dynamic Strings are retained by the Plugin, but are still passed to the SA Prime for Log retention]
- External Source SA System ID
- Connection/Session ID/Request Number
- End User Login Name (or other Unique Identifier for the End User for that particular External Source that was previously passed to the SA system
- SA System ID for applied Access Authorization
- Code indicating Results of Authentication
- Code to indicate whether or Not Plugin to perform redirection
- If Plugin WILL handle Redirection utilizing STATIC variables, the following information is required [Note: If DYNAMIC variables used, plugin has retained these and they do not need to be passed back]:
  o If STATIC URL:
    ▪ URL to Redirect to based on result of Authentication
  o If STATIC String to be passed
    ▪ String to Pass based on result of Authentication
- Hash Value

Passed Information Requirements: Plugin to Source

Results from Authorization Request (Source to handle redirection)
- External Source SA System ID (Validation)
- Connection/Session ID/Request Number

111

- End User Login Name (or other Unique Identifier for the End User for that particular External Source that was previously passed to the SA system
- SA System ID for applied Access Authorization
- Code Indicating Results:
- "1" – Bad
- "2" – Not Found
- "3" – Good

Passed Information Requirements: End User Browser to Plugin
- [Content dependant upon type of device]
- IP of User

Within the Smarte System™, MoveMoney had a need for a viable, cost-effective two-factor end-user authentication solution to secure its own e-payment infrastructure platform, Smarte Pay™, from front-end identity assumption. Available market solutions were either too cost prohibitive or too cumbersome from an implementation perspective to suit the platform's specific needs. As a result, MoveMoney™ began to develop its own authentication solution, eventually known as Smarte Authentication™, for integration into Smarte Pay™. The success of the Smarte Authentication™ concept was dependent upon the development of a physical authentication device that would be suitable for mass deployments to millions of end-users. The best possible device format was the CD-ROM as it offers both extreme affordability and wide-scale availability for end-user use. Of course, integrating a strict anti-forgery mechanism into the device media would be key to making CD-ROMs a viable end-user authentication vehicle. MoveMoney™'s research and development efforts in this area produced a unique media-based copy-protection and embedded serialization technology that is used in its own CD-ROM end-user authentication devices. MoveMoney™ extends this anti-piracy technology for industry-wide use by software developers and manufacturers.

112

Product Authentication, is a set of tools that is provided to Software Manufacturers in order to primarily assist in combating/eliminating moderate to large scale piracy of software distributed via CD-ROM or the Internet (electronic distribution). Product Authentication is designed to allow software manufacturers the ability to prevent medium to large-scale piracy of their programs when either a CD-ROM or the Internet is the distribution vehicle. Note that there are certain modifications required by the software manufacturer to make this a truly effective method of anti-piracy, however the methodology portrayed here can be only partially implemented depending on desired outcome and requirements. One of the primary basic premises that the software manufacturer must make to have this methodology become effective is that they WILL have to make coding changes to the software itself at some point, in order to FORCE the user of the software to REGISTER the software, preferably, on-line via the internet. Current Anti-piracy methods completely fail, as even copy-protected CD's can be remastered/duplicated, and even the best protection can in many ways be FORGED. For example, Microsoft issues a CD "KEY" that must be entered when the software is installed. However, a set of byte for byte replicated disks, along with a written reference to the CD Key that was provided with the originals, is all that is required to have a fully functional "original". Another method that is currently employed, is that the original CD is required to be present in the CD drive DURING the program operation, however, this again fails as a "remastered" CD in virtually all cases is enough to allow the program itself to operate. It is what is known as "Shareware", which has been around for many years, that has actually provided part of the answer here. Shareware, typically, is a program that is designed to be freely distributed, however within the program itself, there are either certain feature limitations, or a "system fail" date/time period, which essentially allows a user to "try" the system for a specific period of time. When the User REGISTERS the software, they are given a "registration code", of which receipt and entry of the code into the registration screen of the software UNLOCKS the software. If the Software manufacturer were to adopt a similar principle in their "standard" issued software packages, REQUIRING registration, coupled with the unique serialization of the distribution

113

media, can virtually eliminate Piracy of the software. In addition, where the distribution software contains MULTIPLE CD's, ALL of the CD's within the individual installation "set" can be set to contain the same anti-piracy features as the initial CD, along with the SAME serial number for each CD within the specific installation "set", making it even more difficult to duplicate/re-master ANY of the installation set CD's. There is also to be supplied a "manual" entry/access screen for the software manufacturer in order to manually work with registrations as well. The MoveMoney™ Security Server retains a listing of the Serial Numbers assigned to all of these individual CD's. In doing this, when the software is registered, that Serial number is then recorded. Since the serial numbers are now tracked statistically, this gives the software manufacturer the ability to set a "registration" threshold setting within the system. Since validation response is aware of this threshold, the MoveMoney™ Security Sever can then respond back to the Software Manufacturer Registration web site (via the Plugin) or manually (via the GUI) the results of the validation. Since the limitations are themselves embedded within the Manufacturer's code, and can only be unlocked via the registration number issuance (which can actually be based on an algorithm to match the individual Serial Number) as well as a consistent factor that changes, such as an embedded value representing the System date, which therefore makes every installation registration code unique. Again, the level of prevention is completely up to the Software manufacturer, however MoveMoney™ now can provide them the means to accomplish this. The basic flow of the Product Authorization system, as used to it's full extent/capability, is shown in FIG. 39.

Smarte Product Authentication™ offers software manufacturers/publishers a flexible and cost-effective piracy management infrastructure and is ideally suited for the protection and promotion of multi-license enterprise software as well as individual consumer-licensed applications distributed on CD-ROM. For product and business environments that do require a rigorous 'anti-piracy' solution, Smarte Product Authentication™ can provide the strictest possible protection to an application distributed on CD-ROM, eliminating virtually all common piracy of the product. Smarte Product Authentication™, though, differentiates itself from

114

alternative anti-piracy solutions in its flexibility of implementation. Because the infrastructure is comprised of four distinct tools that can be used in different combinations and with variable underlying strategies, the resulting piracy management can be tailored to fit company and product specific user base objectives. By uniquely managing piracy through Smarte Product

5   Authentication™, software companies can exploit piracy to their economic benefit - maximizing piracy's positive contributions and minimizing its negative effects. Because the piracy management tools do not require additional hardware or devices, MoveMoney™ can enable an extremely sound, cost-effective and mass-deployable solutions.

Piracy Management Tools Offered through Smarte Product Authentication™

10   *Flexible Copy Protection*

Through a media manipulation technology, MoveMoney™ protects software applications distributed on CD-ROM media. MoveMoney™ offers software manufacturers a cost-effective anti-piracy solution that resides entirely within the CD-ROM media itself. This base level of anti-piracy technology distinguishes the contents of an original, properly licensed CD-ROM

15   from a forgery. With this solution, software manufacturers can effectively render unusable virtually any forged application CD-ROM. Alternatively, this solution allows software manufacturers the flexibility to rigorously protect certain features and/or applications while freely allowing the re-distribution of other features and/or applications contained on the same CD-ROM.

20   At the point of product production (either replication or duplication), MoveMoney™ alters the CD-ROM media by defecting a portion of a known file in a way that cannot be duplicated or digitally reproduced by most CD-ROM writer hardware and software. MoveMoney™ has developed the necessary code for integration onto the CD-ROM media whereby the originality of the CD-ROM can be efficiently validated. MoveMoney™ encrypts

25   and embeds this code during production of the product CD-ROM. The application to be protected can be developed with calls to this originality validation routine. The technical

parameters of the routine (a DLL) are made fully available to the client's development team(s) to ensure seamless use of this tool. The DLL can be called at whatever point or points a particular application needs to validate the originality of the CD-ROM. When called, the DLL either confirms that the CD-ROM is a valid, original CD-ROM or determines that it is a not a valid, original CD-ROM. This key information is then passed back to the application, which would then carry out the appropriate action in line with the software manufacturer's piracy management objectives. Knowing that the media is a valid original or an illegitimate copy provides great flexibility to the manufacturer of the application to do any of the following based on that key knowledge:

- Allow a complete install plus a marketing driven bonus (in the context that the bonus would provide something to a legitimate purchaser that would not be made available to the pirate user).
- Allow a standard complete install.
- Block an install effectively rendering a pirate copy useless.
- Allow a time based install that would render the application useless after a certain period of time.
- Allow only a partial install of the application effectively limiting its use (until, perhaps, the pirate user legitimately registers and pays for full use of the copy).

Embedded Product Serialization

MoveMoney™, also at the point of product replication or duplication, can uniquely encrypt and embed an identifying serial number within the content of each individual product CD-ROM. As an extension of this procedure, MoveMoney™ has the ability to add essentially any other unique content desired by the software manufacturer (such as company specific serial numbers) to individual CD-ROMs. The uniqueness that serialization provides to an individual CD-ROM makes the product a traceable identifier of the original purchaser. Product serialization provides the basis by which use of an individual product (whether its an original or a duplicated copy) can be tracked and managed via the Internet.

Internet-based CD-ROM Reads

As piracy management allows for the individualization of distributed software products, the tool developed to take advantage of this capability is an Internet-based product read. Through any standard web-browser, the serial number can be read from the CD-ROM and, therefore, tracked. Foreseeable online interactions between the product user and the software manufacturer naturally involving the product CD-ROM include online registration of the product, product upgrade downloads, product patch downloads, product documentation downloads, customer service inquiries, license renewals, license upgrades, payment to render a pirated copy or feature 'legitimate', and use or unlocking of any marketing 'extras' the software manufacturer may choose to include with the product.

Beyond providing the link to track the use of individual product CD-ROMs, this tool facilitates the use of serialized CD-ROMs as user authentication access keys in direct support of a web-based direct sales model. The product CD-ROMs can, in effect, become unique identifiers for individual purchases made during future Internet based transactions conducted through the software manufacturer's (or designated agent) website. As an authentication key, serialized CD-ROMs serve to protect the online identity of the purchaser as well as provide the software manufacturer with strong transactional non-repudiation (protection against Internet-based identity fraud).

The full product purchased by the customer could contain several applications in addition to the intended purchase. Even though burned as full products onto the CD-ROM, these additional applications could be presented to the customer in limited formats such as demo packs or trial versions. Accompanying license information could also be bundled with these additional applications. The customer could then choose to directly purchase any of these additional products (via the Internet). At the time of purchase, the software manufacturer would generate and return to the customer a digital key (based upon the serial number contained within the CD-ROM, a time factor, and a factor unique to the software manufacturer) in conjunction with the presence of the CD-ROM itself to unlock the application and its appropriate license.

117

A Utility for the Protection of Downloadable (electronically distributed) Applications

MoveMoney™ can provide the necessary infrastructure (an enhanced Dynamic Link Library) to generate a unique authorization code (an encrypted number) based on elements taken from each of the following: the unique serial number contained in any MoveMoney™ serialized CD-ROM possessed by the customer, a time factor, and a factor unique to the software manufacturer. The validity of this generated authorization code can be time-limited (by date, for instance) to prevent its unauthorized sharing with respect to the application it serves to unlock. The customer would then use this authorization code (within the specified time limit) in conjunction with the serialized CD-ROM to enable an install of the application. Beyond the act of installation, the software manufacturer could further support the integrity of the application with other piracy management tools such as Internet-based installation tracking and/or additional CD-ROM originality validation checks during use of the product. Because Smarte Product Authentication™ strongly supports the protection of electronically distributed software, use of the CD-ROM as a primary source of product distribution can be eliminated.

Marketing/Sales Opportunity Enablement

MoveMoney™'s CD-ROM serialization and protection methodologies enable the software manufacturer to be as creative as possible when distributing or marketing software products. Some marketing applications enabled by Smarte Product Authentication™ are outlined in the following:

Bundling of Products on Distributed CD-ROMs

The software manufacturer can bundle any combination of full products, limited-use versions, trial versions, demo versions, and license packs on the same CD-ROM (capacity-limited) or set of CD-ROMs. These product types can be distributed in conjunction with purchased applications or simply as enticements to purchase. Customers or potential customers can easily and efficiently purchase and register the product online through the software manufacturer (or its designated agent) as well as receive the means necessary to gain access to the purchased application.

118

Increased Online Customer Interaction

Several piracy management features could promote the online interaction between the software manufacturer and its customers. Increased online interaction translates into increased direct sales opportunities as well as increased knowledge about the user base, which can then be used to further enhance marketing strategies.

Regional Product Targeting

The software manufacturer can develop and distribute product bundles based on regional demographics and competitive landscapes.

Application Rentals

The use of piracy management tools enables the rental of applications and application licenses both through electronic distribution and through traditional brick-and-mortar outlets. As the tools provide for use-of-application tracking and control, software rental marketing schemes become viable, protectable options for the industry.

Eliminates the Need for Easily Re-distributable License Diskettes (Enterprise Software)

Because multiple unique content files can be embedded within product CD-ROMs, piracy management can be used to eliminate the need for enterprise software manufacturers to use floppy diskettes as the (unprotected) medium for distributing license related serial numbers and encryption keys.

The CD-ROM containing the enterprise application can be burned with the necessary enterprise license related serial number and unique encryption key in addition to MoveMoney's unique serialization of the CD-ROM. In this manner, the CD-ROM would become the only media the enterprise customer would need to maintain as it contains both the application and the necessary license information.

The unique license information can be burned on a MoveMoney™ serialized CD-ROM separately from the application. This would, in effect, replace the enterprise software manufacturer's current use of the floppy with a MoveMoney™ protected CD-ROM. The enterprise customer would still maintain an application CD-ROM along with another CD-ROM

119

containing the license information for that application. This scenario would enable the application CD-ROM to still be burned without MoveMoney™'s media manipulation and, thus, allow it to be archived by the customer.

Even though protected from unauthorized copying, original license-containing CD-ROMs would still be vulnerable to 'sharing' between companies without further protocol. MoveMoney™ piracy management technology can be used to track the number of installations by unique product serial numbers. This would require an online interaction (perhaps during product registration) between the application manufacturer and the legitimate purchaser of the product in order to record the application's legitimate installation. With this knowledge, the manufacturer can choose to deny further installations of the same original product beyond legitimate customer service related issues.

Separately or in addition to installation tracking, the software manufacturer could choose to require a simple media originality check to be performed by the enterprise application to ensure the user owns a valid, original license and/or application. These checks could be required periodically (weekly or monthly, for instance) and/or the software manufacturer could choose to require the original CD-ROM to present during general or particular use of the enterprise application. Failure of these checks could be programmed to result in time-delayed termination-of-use of the enterprise application.

Large Scale Product Replication/Individualization

Using a hybrid replication/individualization technology in conjunction with MoveMoney™ developed management software, the large-scale and highly cost-efficient process of producing serialized product CD-ROMs can be conducted by the production house(s) of the software manufacturer's choice. Alternatively, MoveMoney does have the capacity to act as a serialized product CD-ROM production house.

Efficient large-scale replication of individualized product CD-ROMs involves a three-step process:

120

The software manufacturer would supply an import file to the production house containing all unique licensing information (and/or other unique information such as the software manufacturer's product specific serial numbers) that can then be directly read into MoveMoney™'s replication management software along with any common content (the application files, for instance) to be burned onto all CD-ROMs in a particular batch.

All content common to a set of product CD-ROMs is replicated (stamped) from a glass master. A small portion of the CD-ROM media is left open (available for a single post-stamping write to the CD-ROM) for all individualized content.

The CD-ROMs containing the common content are then sequentially written to with the necessary unique content supplied by the software manufacturer (from the import file), the copy protection mechanism, and a MoveMoney supplied serial number (encrypted).

For non-serialized CD-ROMs containing only the media-based copy protection, the functioning of MoveMoney developed replication/duplication software is depicted in FIG. 90. The functioning of MoveMoney developed replication/duplication management software is depicted in FIG. 91 for single set serialized CD-ROMs and in FIG. 92 for sets of serialized CD-ROMs.

Implementation of Piracy Management

Two essential processes would be involved in implementing MoveMoney™'s piracy management technology:

At the marketing level, the software manufacturer would determine how to use MoveMoney™'s piracy management tools within its products/licensing structures to best support its anti-piracy and marketing objectives.

At the application development level, calls to the piracy management tools would be embedded within the product code along with the necessary logic to instruct the application to act accordingly, based on the information the piracy tool(s) pass back. The software manufacturer would determine where and how frequently the use of the piracy management tools occurred within a given application, to best support piracy management objectives.

121

Elements of the Smarte Product Authentication™ piracy management platform are depicted in FIG. 97.

Enterprise Software Authentication™

Enterprise Software Authentication™ is a tool that enables enterprise software developers to effectively and efficiently create, as a value-add feature, a sound device-based user authentication infrastructure within access sensitive enterprise products. The end result of the methodology gives the enterprise customer the ability to secure access to its software application with strong two-factor user authentication, combining 'something the user knows' with 'something the user physically has' – all without the need for drivers or additional support software.

The devices, which provide the definitive layer of user authentication, are uniquely serialized mini-CD-ROMs, Smarte CD™s. The CD-ROM format delivers affordability, convenient portability, security against forgery, branding opportunities, and complete end-user privacy (no personal information is required).

With this feature, an enterprise software purchaser has a significantly improved ability to effectively manage and control internal access to the software application. Enterprise User Authentication is a strong value-add feature in software application environments where strict access control to the application itself and/or data generated through the application is of prime importance to the business or organization using the application.

Enterprise software application types that would naturally benefit from this user authentication feature include:

- Sales & Distribution
- Accounting
- Investment Management
- Materials Management
- Human Resource Management

122

- Quality Management

- Database Management

- Project Management

- Network Management

5   - Production Planning

MoveMoney provides the manufacturer of the software with the necessary tool around which a strong user authentication infrastructure can be built within an application. This tool is essentially an 'Extended DLL Plug-in', which serves to create and manage data files governing the user and associated authentication device information. FIG. 75 depicts a diagram displaying

10   the Extended DLL data file structure. FIG. 77 is a flow chart depicting the basic functional flow of the Extended DLL. An application developed with the Enterprise Software Authentication tool can be delivered with a software-based switch that allows the enterprise customer the option to use or not to use the Enterprise Software Authentication feature. The CD-ROM user authentication credentials can be delivered at the point of sale of the application or at any later

15   date when the enterprise customer chooses to use the feature. Upon the decision by the enterprise customer to use the device-based user authentication feature (and receipt of the devices themselves), the DLL Plug-in, in the context determined by the application developer, provides the means necessary to effectively manage the application's authorized enterprise user base.

Because it is specifically designed as a tool for use at the application development level,

20   the software developer can shape the use of the DLL Plug-in to fit the exact user base access management needs of the enterprise product.

Functions provided by the Extended DLL Plug-in relating to application-driven user authentication are outlined in FIG. 78, FIG. 79, FIG. 80, FIG.81, FIG. 82, FIG. 83, FIG. 84, FIG. 85, FIG. 86, FIG. 87, FIG. 88, and FIG. 89. The Enterprise Software Authentication user access

25   management platform using the Extended DLL is depicted in FIG. 95.

The Smarte CD™

123

The Smarte CD^{TM} may have any or all of the validation and serialization methodologies applicable, depending on the CD usage. For example, for User Access Authentication, ALL of the methodologies may be employed, however, for Product Validation, only some of these methodologies may be opted to be used by the supplier of the software. The validation process for the Smarte CD^{TM} is displayed in FIG. 40.

5

Like the Smarte CD^{TM}, there is a specific validation flow for the Smart Card, as shown in FIG 41. Unlike the Smarte CD^{TM}, however, the Smart Card is used solely for User Authentication, and therefore the validation process and methodology for the Smart Card is fixed.

10

The specific validation flow for Third Party Devices is as shown in FIG. 42. In this case, it is the Smarte Authentication^{TM} portion of the Smarte System^{TM} that interacts with the external authentication server or software. In FIG. 42, this validation flow is displayed. In FIG. 42, the external authentication mechanism is displayed as a separate physical server, however it could easily just as well be a program running in the background on MoveMoney^{TM}'s own servers.

15

This flow is valid regardless of physical proximity or location to the MoveMoney^{TM} servers, the requirement only being a clear and secure communications channel to exchange information. FIG. 43 uses the RSA^{TM} ACE^{TM} Server as an example, to display a "typical" set-up, include recommended "hardware" involved. Note that this structure is defined on MoveMoney^{TM} itself maintaining the ACE^{TM} server, and allows for users to utilize RSA^{TM} devices without having to register within the Smarte Authentication^{TM} system, going DIRECTLY to the ACE^{TM} Server.

20

The basic flow for the Authentication Process is represented in FIG. 44. MoveMoney^{TM} receives purchased devices/device media, and adds to inventory as required dependant upon the type of device. Depending on the device type, one of the following will apply as applicable:

- MoveMoney^{TM} Generates Serialized CD's From Inventory

25

Import Listing of Serial Numbers, SN Strings, Volume Labels, etc.

Option to ADD as individual items or apply against existing inventory

- MoveMoney^{TM} Generates Serialized Smart Cards from Inventory

124

Import Listing of Serial Numbers, SN Strings, Volume Labels, etc.

Option to ADD as individual items or apply against existing inventory

- MoveMoney™ 3rd party devices as required

Following the devices being placed in inventory, MoveMoney™ issues the devices to the

5 External Authentication Sources for Distribution to End Users and/or Internal Use. MoveMoney,

utilizing the Authentication Issue Screens issues the devices to the applicable External Source

either by Lot, Device Serial Number Range, or SINGLE device. This results in "ownership"

transfer to the applicable External Source. The External Source, retains ownership even after

assigning a device to an End User, as it is the External Source who retains control over the

10 device and the options for that device. As the Device Ownership is conferred, so to is Complete

Device Control Authority for each of the devices Issued.

From this point, the External Source receives the devices from MoveMoney™. It is up to

the External Source how it wants to physically distribute devices to its end users – through mail,

in person, or by 3rd Party, for instance.

15 The External Source will Attach Access Authorizations to each device. This can be done

individually or in a "bulk" group (many selected Authorization Masters against many individual

devices) as needed.

Once the devices have been distributed to the End Users, the External Source "Activates"

the particular device manually in system, entering any applicable back-up information as

20 required based on the activation.

Another mechanism for activation of a device that can occur is where the End User

"Remotely" activates the device, based on additional information sent to them, personal

information previously known to the External Source, or a combination of this. In this case, the

End User performs this activation of the device via entry into a "special" area of the Smarte

25 System™. The basic flow requirements for this are as follows:

- End User "Activates" Device Automatically

    o End User receives and physically has the device in their possession.

125

o   End User is provided a URL to go to for automatic device activation.

\-   End User goes to the URL provided [EUAS01, EUAS02] and is prompted for device specific information (serial number printed on the device).

\-   End User enters the device specific information

\-   IF the device is found, THEN the End User is prompted for their identifier information.

\-   End User enters their personal identifier.

o   If personal identifier is a correct match, THEN the system activates the device. The End User is given confirmation that the device has been activated.

o   ELSE the End User is re-prompted for their personal identifier. [This occurs three (3) times at the most.]

o   ELSE the End User is given a message that their device is not activated and to contact customer service.

Still another mechanism for activation is where a 3rd Party "Activates" Device Manually. This can be done where the External Source has either no desire, infrastructure, and/or resources to perform the activation. The system allows the "owner" of a device to extend specific authority for actions and control to other External Sources. Note that also extends to the assignment of devices to End Users as well. The basic process is as follows:

\-   End User receives and physically has the device in their possession.

\-   End User was provided contact information with the device regarding 3rd party Activation of the Device.

\-   End User contacts the 3rd Party/3rd party Contacts End User

\-   3rd Party User Logs into the Smarte Authentication^{TM} system.

\-   3rd Party User goes to the End User Activation screen.

\-   3rd Party User retrieves the device number (printed on the device) from the End User.

126

- 3rd Party User enters the device number.

- IF device is found, THEN 3rd Party User retrieves the personal identifier information from the End User.

- 3rd Party User enters the personal identifier information.

5   - IF the personal identifier matches, THEN the device is activated.

    o 3rd Party User is given confirmation that the device is activated.

    o 3rd Party User notifies the End User that the device is activated.

- ELSE, the identifier does not match,

    o 3rd Party User is given screen notification that the identifier does not

10   match.

    o 3rd Party User notifies the End User that the personal identifier was incorrect.

- ELSE, device is not found,

    o 3rd Party User is given screen notification that the device is not found.

15   o 3rd Party User notifies the End User that the device number is not valid.

There is an additional option during Device Assignment to an End User, whereby the Device can also be Activated at the same time as Assignment by the system. This is used primarily where direct physical contact and physical identification of the End User occurs.

20   For an External Source to Transfer Device Ownership, it must first hold Device Ownership.

Device Ownership can be Transferred either in groups by Lot or Serial Number Range. The External Source User chooses the method by which Device Ownership is to be Transferred. Based on this choice, the External Source User goes to the Transfer Lot screen or Device S/N

25 Range Transfer screen. Here, the device(s) to be Transferred are selected (by Lot or Serial Number Range). The system prompts the External Source User for the External Source ID to which Device Ownership is to be transferred. The system checks that the External Source from

127

which Device Ownership is to be transferred does, indeed, hold Device Ownership for the selected device(s). For any breaks in the master series (breaks defined as Device Ownership not held by the External Source), the system generates new Lot designations for unbroken sub-series existing within the master series. The system then Transfers Device Ownership to the new

5 External Source by any new Lot designations created.

The system must remove all Device Control Authority for all Device Ownerships Transferred from the original External Source. Since Device Control Authority is validated at the External Source Level, there is no direct affect in any data tables concerning this. Once ownership the ownership transfer is completed, any Device Control Authority granted to other

10 External Sources by the External Source having ownership of the devices is automatically applied. Upon completion of Transfer, all Device Control Authority now rests solely with the destination External Source.

Any External Source that holds Device Ownership retains Complete Device Control Authority, regardless of whether any or all Device Control Authority is Granted to another

15 External Source.

Granting of any Device Control Authority can only occur from the holder of Device Ownership to another External Source, i.e. the External Source receiving the Grant of Device Control Authority cannot further delegate that authority to another External Source. The External Source holding Device Ownership can, however, Grant the same type of Device Control

20 Authority to multiple External Sources. To Grant Device Control Authority, the system must know the Devices for which Control Authority is being Granted (by Lot or System Serial Number), the ID of the External Source to which the Device Control Authority is being Granted, the ID of the holder of Device Ownership, and the specific types of Device Control Authority being Granted. The system should check that the External Source that is Granting the Control

25 Authority is, indeed, the holder of Device Ownership for the selected devices. To Grant, the system must extend those chosen management rights for the selected devices to the designated External Source.

128

Individual Devices are assigned to an individual End Users using one of the following methods:

- Via Plugin Specified as Single Device/Device Type Only (Fixed Source). Login is routed via Smarte Authentication™ Plugin. Plugin acts simply as portal for information to pass. All validations of acceptance/rejection performed on MoveMoney™'s Security Server.

- Via Plugin Specified as Multiple Devices/Device Types (Fixed Source). Login is routed via Smarte Authentication™ Plugin. Plugin acts simply as portal for information to pass. All validations of acceptance/rejection performed on MoveMoney's Security Server.

- Via Plugin (Smarte System™ Login). Login is routed via Smarte Authentication™ Plugin OR Plugin "simulated" code as part of Smarte System™ itself. Plugin acts simply as portal for information to pass. All validations of acceptance/rejection performed on MoveMoney's Security Server.

Elements of MoveMoney's Smarte User Authentication identity management platform are depicted in FIG. 94.

ACCOUNTS AND PROCESSING REQUIREMENTS

The Smarte System™ maintains multiple account types and is structured such that additional accounts types can be added to the system without an appreciable impact on the existing system in regards to redesign or restructure. The primary functional account types are detailed, however the system is not limited to these types of accounts.

Each of the various accounts, as well as the nature of the action against the account, requires specific actions which may require that multiple transactions be generated against other accounts, which in turn may have a recursive effect on transaction generation.

129

Administrative Accounts are "theoretical" accounts within the system that act to identify the ownership and origin of amounts of funds where the actual money is "pooled" together into a single "physical" account, such as a corporate checking account. Administrative Accounts will always reference a physical account of this nature. Administrative Accounts may also be used as "holding" accounts for funds that are pending transfer via the transaction process, or that are being delayed in their transfer due to settings or prior agreements in order to mitigate risk.

The Reserve account is maintained at the individual Product Class Level. There is only a single Reserve Account for each Product Class, and all Product Classes have this account created as an inherent part of the system. The purpose of the Reserve is to provide a "safety net" of funds from the individual Sellers against the various product classes in the event that Returns are received AFTER the Seller has been reimbursed fully for a particular batch. The "balance" of a batch, in lieu of funds to be reimbursed to the Seller, is essentially as follows: + (Absolute value of Total Amount of Applicable Debit Transactions) – (Fees) – (Reserve Calculations) – (O&A Amounts). This is the amount to be reimbursed to the Seller against a Batch during Payment Processing. For example, assume that the amount then to be reimbursed to the Seller has been paid in full, and therefore the result of the above formula is now $0.00. Assuming after this point, a RETURN is received, for which there is no resubmission/redress. Where this is the case, this amount is therefore uncollectable, and the Seller must bear the amount of the Return. Since the balance of the Batch prior to this return was $0.00, this new return drives the balance of the initiating batch to a negative balance. In addition to the amount of the return transaction itself, this amount is driven to a further negative amount by any Fees levied against the Seller for the receipt/processing of the return. It is ONLY in this scenario (Batch Balance =<$0.00) that the funds are removed from the RESERVE ACCOUNT, in order to offset the amount owed back to MoveMoney. These funds are then directed to MoveMoney's account. By allowing the "split"/delayed reimbursement under Product Class much of this is mitigated by holding back some of the reimbursement funds. Now, as further clarification of the O&A amount: This occurs when there is insufficient balance in the applicable Seller's RESERVE account to accommodate

130

the total of the Returns. In this scenario, after the Product Class Reserve Account has been "drained", the money owed is then subtracted from the Next subsequent Batches where reimbursement amount owed to Seller is still greater than $0.00. In the event that a Return transaction, such as an NSF transaction is resubmitted, the following rules apply:

5   -   The original (parent transaction) amount is reversed from the amount to be reimbursed to the Seller.

-          If the amount of the return drives the Batch balance to below zero (negative amount), the rules as previously described apply.

-          Fees are NEVER backed out in this situation. Commissions ARE reversed ONLY when a RETURN is declared NOT to be collectable (new transaction NOT generated).

-          The resubmittal transaction is Generated as a NEW transaction, along with (Smarte) a new BATCH record as/if needed against the applicable Product Class.

-          The NEW generated transaction References the Original/Parent Transaction in the table.

-          The Original/Parent Transaction record is updated to reflect the NEW transaction generated in the table.

Commissions are NOT generated for resubmitted transactions. Additional Fees ARE generated at the BATCH and ACH TRANSACTION LEVELS only, as any additional fee application would be considered "double-dipping".

Smarte Cash™ is a reserve of money set aside by the individual Buyers that is used to Purchase (via the Smarte System™) over the internet. This money is directed to a "pool" account, and the Sellers are paid from this pool account. All accounts and balances are maintained by the Smarte System™, thereby removing the requirement for any external source to maintain additional or modify existing programs. Under this scenario, the funds are "guaranteed" to the individual Sellers. This type of Smarte Cash™ account is referred to as

131

TYPE I. Another mechanism in which Smarte Cash™ may become available to Buyers is through a "special" system whereby a Depository type Financial Institution permits some or all of the principle or interest from a Certificate of Deposit (CD) account to be utilized by the Buyer for purchases. This type of Smarte Cash™ account is referred to as TYPE II. Type II is

5   structurally/functionally different than Type I in that only a PORTION of the account balance may be available to the Buyer for use in purchases. Funds can be diverted from existing accounts set up within the Smarte System™, or they can be entered directly by MoveMoney™ or the individual participating entity. Originally, the concept would be ONLY MoveMoney™ and Banks that could allocate funds, but this can also be extended to "Paycheck/Cash Advance"

10   Houses as another feature they could offer in order to get them into the Internet world as well. These types of "Smarte Cash™" accounts are NEVER intermixed. TYPE is maintained as a value within the System in order to differentiate them. Since the Smarte Cash™ System is to be managed through a series of "pool" accounts, the issuing entity for the initial credit must be a financial institution. Note that under the SYSTEM STRUCTURE definitions, a Financial

15   Institution is NOT limited only to banks, but can be virtually any entity. MoveMoney™ is also be set up in the system as a Financial Institution itself, as it is handling money in a "pool" type reserve as well. Financial Institutions do NOT require an RTN to be part of the Smarte System™. An individual RTN is only required for a Financial Institution to operate as an ODFI through the ACH process, or is of the Financial Institution type "Bank" (including Credit

20   Unions). An RTN IS required for all ACH account transactions. An additional feature that is unique to the Smarte System™ is the utilization of this system by Buyers to Sub-Buyers. This would most likely impact the Parent/Teen market, as Parents can allocate funds to Sub-Buyers (children) directly through the MoveMoney™ System. In this manner, it also allows the parents to monitor their children's purchases over the web. Buyers are NOT limited to a SINGLE Smarte

25   Cash™ account per Individual, as they may sign up with more than one issuing Financial Institutions. A Buyer MAY also allocate from the Smarte Cash™ account to Sub-Buyer's Smarte Cash™ Accounts PROVIDED IT IS UNDER THE SAME ACCOUNT, or to pay off Smarte

132

Credit™ Balances. A Buyer may NOT Transfer balance amounts between individual Smarte Cash™ Accounts, as this creates a "balancing" problem between the Smarte Credit™ system and the individual issuing Financial Institution accounts. The basic System Flow for the Smarte Cash™ system would be as follows:

- The Buyer initiates a Smarte Cash™ Balance within the Smarte System™ by transferring Money from a personal account (either on-line) or through the Smarte System™ itself.

(or)

Third party initiates the account balance through pre-arrangement with MoveMoney™ (Set-up of bond, etc…)

(or)

Depository type Financial Institution creates Smarte Cash™ balance based on released amount of Buyer CD Account Principle/Interest.

- If performed via the Smarte System™, the transaction is processed as required and the money is moved to the applicable Issuing F/I's (regardless of FI type) Pool Account.

- If performed by the Issuing F/I, they take the money and manually increase the balance of the Buyers Smarte Cash™ account through the Smarte System™, indicating also how much time the available amount was to be held. In this manner, If the buyer walks into their bank and transfers funds from an existing account at that bank, the bank has the option to immediately release the funds, as they have direct control over the draw account.

- The Buyer's account also acts as a form of "guarantee against transactions made using other Accounts. For example, if the Buyer opts to use their standard Checking Account while a balance is maintained within the Smarte Cash™ Account, the Buyers Smarte Cash™ Account(s) would

133

immediately be debited for the amount of an NSF transaction. If the Buyer goes negative, the "issuing" Financial Institution assumes the risk until proper collection of the funds can be collected from the Buyer. This risk is that the funds are removed by MoveMoney^{TM} from the Sponsoring Financial Institution's Pool account. If the FI IS MoveMoney, then MoveMoney^{TM} assumes the risk.

As part of the standard agreement with the Buyer, in order to cover the issuing Financial Institutions (including MoveMoney), it must be noted to the Buyer that the Issuing Financial Institution has the right to attempt to collect "overdrawn" funds from other specified accounts electronically as/if needed. In order to avoid the majority of the potential NSF situations that could arise, a mechanism for a "hold" on the availability of the funds is incorporated. This mechanism on Funds availability works in conjunction with the Funds availability system in the Smarte Credit^{TM} system. This "hold" is at the discretion of the issuing Financial Institution, allowing them the opportunity to determine the amount of risk that they wish to assume on transactions of this nature. In the event of a Buyer Revocation of Authority, the amount is allocated from the Buyer's account (frozen) until the issue can be resolved).

The Automated Clearing House (ACH) process is the primary core transaction-processing feature of the Smarte System^{TM} and is directly linked to the Smarte Credit^{TM} Account Process. It functions on the same level as an individual manually writing a check against a checking (or savings) account with a Bank (or Credit Union). In order for the ACH process to occur, the account specified must be a valid checking or savings account. While the process of creating and submitting the ACH transaction is fairly straightforward, the ability to handle and manage returns effectively is a much more complex model. ACH transactions may be returned for a variety of reasons, and the Smarte System^{TM} utilizes Return handling processing concepts in order to accommodate this condition. Since all transactions are a direct result of a payment action, the Smarte System^{TM} itself handles the transaction generation. However, because of the complexity of the return process, direct user intervention is often required.

134

Smarte Credit™ is a form of "guaranteed" payment, whereby the sponsoring Financial Institution (Bank) enters a pre-approved "loan" amount for a Buyer into the system, directly attached to a specific Account maintained for the Buyer (Checking/Savings). This amount is ONLY activated if the Buyer performs a purchase where there is an insufficient amount of funds

5   within the applicable account to cover the total amount of the transaction. At this time, the Buyer's Smarte Credit™ account would cover the TOTAL amount of the purchase in the form of a "loan". The sponsoring Financial Institution maintains control over the available amount of, as well as percentage charged for amounts in the Smarte Credit™ account. An additional aspect of the Smarte Credit™ Type of Account against a SPECIFIC Account as initiated by a Financial

10   Institution, MoveMoney™ may issue a "general" Smarte Credit™ type of Account which acts primarily as general "insurance" or overdraft protection against all of the Buyer's accounts in general. In this type of Smarte Credit™ Account, ONLY MoveMoney™ can acts as the sponsor. MoveMoney™ issues the amount to cover the NSF from it's internal pool account, however there is no interest charges accumulated for this, only an "activation" fee. The buyer then has 30

15   days from the time of the processed "NSF covering" transaction with which to pay off the balance IN FULL to MoveMoney. If not, then MoveMoney™ can assess an additional late charge, or attempt to collect electronically from one or more of the Buyer's other accounts. An additional late fee may be applied, however in this time of account, there is NO interest charged. These two types of Smarte Credit™ Accounts cannot be intermixed and are kept as separate

20   accounts, although any single buyer may have multiple Smarte Credit™ accounts or various types under them. Smarte Credit™ ALWAYS applies the PARENT buyer (in a Buyer & Sub-Buyer Relationship). Allocation of Smarte Credit™ cannot occur within the system. There are two basic ways that the Smarte Credit™ can be activated against an account. The Smarte Credit™ is ONLY activated for the amount OVER AND ABOVE and overdraft protection that

25   the bank may have offered the Buyer that results in an NSF condition. Once the Smarte Credit™ has been activated, the Buyer, upon logging in to his account the next time is notified of the current credit balance. There may be MULTIPLE credit accounts active at any given time,

135

Smarte Credit™ is a form of "guaranteed" payment, whereby the sponsoring Financial Institution (Bank) enters a pre-approved "loan" amount for a Buyer into the system, directly attached to a specific Account maintained for the Buyer (Checking/Savings). This amount is ONLY activated if the Buyer performs a purchase where there is an insufficient amount of funds

5   within the applicable account to cover the total amount of the transaction. At this time, the Buyer's Smarte Credit™ account would cover the TOTAL amount of the purchase in the form of a "loan". The sponsoring Financial Institution maintains control over the available amount of, as well as percentage charged for amounts in the Smarte Credit™ account. An additional aspect of the Smarte Credit™ Type of Account against a SPECIFIC Account as initiated by a Financial

10   Institution, MoveMoney™ may issue a "general" Smarte Credit™ type of Account which acts primarily as general "insurance" or overdraft protection against all of the Buyer's accounts in general. In this type of Smarte Credit™ Account, ONLY MoveMoney™ can acts as the sponsor. MoveMoney™ issues the amount to cover the NSF from it's internal pool account, however there is no interest charges accumulated for this, only an "activation" fee. The buyer then has 30

15   days from the time of the processed "NSF covering" transaction with which to pay off the balance IN FULL to MoveMoney. If not, then MoveMoney™ can assess an additional late charge, or attempt to collect electronically from one or more of the Buyer's other accounts. An additional late fee may be applied, however in this time of account, there is NO interest charged. These two types of Smarte Credit™ Accounts cannot be intermixed and are kept as separate

20   accounts, although any single buyer may have multiple Smarte Credit™ accounts or various types under them. Smarte Credit™ ALWAYS applies the PARENT buyer (in a Buyer & Sub-Buyer Relationship). Allocation of Smarte Credit™ cannot occur within the system. There are two basic ways that the Smarte Credit™ can be activated against an account. The Smarte Credit™ is ONLY activated for the amount OVER AND ABOVE and overdraft protection that

25   the bank may have offered the Buyer that results in an NSF condition. Once the Smarte Credit™ has been activated, the Buyer, upon logging in to his account the next time is notified of the current credit balance. There may be MULTIPLE credit accounts active at any given time,

135

depending upon the number of accounts and Banks under which the individual Buyer has subscribed. Payments against Smarte Credit™ can ONLY be made through the Smarte System™. If the Buyer REVOKES Authorization on the PAYMENT transaction, MoveMoney assumes the temporary liability for the amount until it can be shown to the member bank that it

5 was a valid payment under our current terms. In all cases the member bank assumes the FINAL liability for the amounts. Smarte Credit™ is designed to be a checking/savings account OVERDRAFT protection in the form of a pre-approved loan amount. It is NOT designed as a guarantor of funds in the event of an NSF, as the UNUSED amount is NOT balance controlled against current/recent purchases. The other reason for this is that the consumer would be limited

10 to amount of purchases they could make, regardless of what their checking/savings account balance was. The other limitation in utilizing the Smarte Credit™ as a guarantor of funds was that individuals who were not assigned a Smarte Credit™ limit could not use the system. Therefore Smarte Credit™ is utilized simply as a "back-up", in case the user does have an NSF during the ACH process. The Smarte Credit™ is ALWAYS a 1:1 relationship against a

15 particular account. Smarte Credit™ Accounts NEVER span multiple accounts. Likewise, more than one Smarte Credit™ Account is NEVER applied against another account. There is no "supplemental" Smarte Credit™ accounts against an individual checking/savings account. The Smarte Credit™ account is ONLY applied to Checking/Savings accounts, and is not applicable to Smarte Cash™, Credit Cards, or other types of accounts. MoveMoney™ assists the Financial

20 Institution in supplying them the basic legal context agreement for the Buyer's, which is the "pre-agreement" to the terms of the Smarte Credit™, should the Smarte Credit™ have to be utilized. In essence, this is an "unsecured" cash loan by the bank to the buyer, and legally would fall under those guidelines, regardless of activation mechanism. Therefore, MoveMoney™ maintains a periodic calculation mechanism within the system in order to handle the calculations

25 of interest, as well as payment information, etc. The creation of a Smarte Credit™ Account for a Buyer in the system is completely up to the individual sponsoring FI's discretion. Ideally, the FI evaluates each Buyer and determines, based on their internal criteria (such as credit, avg. account

136

balance, account history, etc.) what amount, IF ANY, to allow the Buyer in the Smarte System™. The Smarte System™ assigns the Smarte Credit™ System Account ID. The Financial Institution enters the account that the Smarte Credit™ is attached to (assuming Buyer already known and attachment to account from a list of available APPLICABLE accounts), as well as the

5   following information:

- Internal Reference for Account (Optional)
- Comments (Optional)
- Total Amount of Smarte Credit™ Available
- Number of Days following Activation to delay Interest Charges

10   - The Financial Institution's OWN Account used to back the Smarte Loan™
- Default Interest Rate for Account
- Flat Rate Fee to add to account as "processing charge/fee" for Activation
- What Day of the Month the minimum payment against the account is due
- Minimum monthly interest charge (flat rate: example: $0.50)

15   - Minimum Allowable Payment Amount (Applicable while Curr Bal of activations > this amount)
- Default Percentage of Total Balance to Calculate Minimum Payment against.
- Whether or Not to waive the (Std) NSF Fee Trans that would typically be

20   charged to the Buyer.
- Late Fee Calculation Information (Additive/ not Exclusive to each other)
  o Flat Rate Late Fee
  o Maximum Late Fee "cap" amount
  o % of Balance to calc late fee from

25 The System calculates/Assigns the following information:
- Sets the next Sequential Loan Number to "1"
- Sets Current Balance to $0.00

137

-       Sets Four Digit Calendar Year to current year.

-       Sets Total Amounts of Interest Paid (current and previous years) to $0.00

Regardless of the activation point of the Smarte Credit™ Account, EACH ACTIVATION is considered to be an INDIVIDUAL LOAN against the account. While the account itself will have a common payment due date, as well as roll up all totals, interest is always calculated individually against each "loan" separately. The FI's Account (that backs the Smarte Credit™ Account) is debited the amount of the TRANSACTION. If A Buyer NSF Fee Transaction is required (ACH) it is processed based on specifications within the applicable Product Class(es). Notifications generated to BUYER, FI, and MoveMoney™ as required. (NOT THE MERCHANT). If Buyer was SUB-Buyer Type, notification also sent to PARENT Buyer. There are Two (2) ways that Smarte Credit™ can be paid down: Manually through FI (or MoveMoney™); or via Buyer action to initiate payment from other account.

In the "manual" scenario, the Buyer physically walks in or mails the money in an acceptable form to the applicable sponsoring FI (MoveMoney™ will not accept payments to Smarte Credit™ on behalf of another FI at this time, but will accept payment IF MoveMoney™ is the sponsoring FI). The FI accepts the payment and handles in standard fashion (e.g.: Cash deposit: cash accepted and credited internally according to current practices). The FI then accesses the Smarte Credit™ Payment Screen for the applicable Buyer, accesses the applicable account, and enters the information regarding amount and reference information/comments as required. In the "automatic" scenario, the Buyer initiates payment from another account with sufficient funds to handle the payment, specifying amount to pay, and from which account. Note that merchant fees do NOT apply in this scenario regarding payments of this nature, nor are commissions levied against the transaction. The transaction is handled in the required fashion based on the TYPE of account that is being used to pay down the balance.

Example: Smarte Cash™ Used.

-       Money debited from Buyer's Smarte Cash™ Account

138

- Money Transferred to Sponsoring FI's holding account (via ACH or credit given for later reimbursement via manual draft/check depending on set-up with Bank).

Example: Smarte ACH™ Used.

- Money debited from Buyer's Checking/Savings via ACH transaction
- Money Transferred to Sponsoring FI's holding account (via ACH or credit given for later reimbursement via manual draft/check depending on set-up with Bank).

In ALL cases, where multiple activations (loans) are active at the same time, the OLDEST loan is paid off FIRST. When individual loan balance is ZERO ($0.00), then any remaining monies are applied against the NEXT oldest.

Smarte ATM™ Transactions are handled via the PULSE network, utilizing PULSE Deluxe ISO 8535 PI Message Structure. Active Communication protocols between the Pulse network and the Smarte System™ are defined. Since ATM functions using ACH compatible Accounts (checking/savings), there is no delineation in the accounts themselves, only in regards to the actual processing requirements that must occur regarding these accounts. Unlike the ACH network, the ATM network processes the Transaction in "real" time, that is that the money is withdrawn immediately from the Buyer's Account (via the applicable Financial Institution) upon processing of the transaction. Additionally, unlike the ACH network, the balance of an individual's account can also be validated immediately prior to processing the transaction itself.

Smarte Credit Card Accounts are maintained in the system in an informational methodology only. No balances are maintained, and all transaction processing occurs via currently available transaction processing portals made available by the various Credit Card Issuing Companies.

TRANSACTION PROCESSING REQUIREMENTS

The basic Structure of Transactions within the Smarte System™ is displayed in FIG. 45. Transactions are defined in two levels within the Smarte System™. The first level is that of the transaction itself, which is the basic requirement for movement of money within the system. The second layer of transactions, are those transactions that ACTUALLY perform the transfer of

139

funds between accounts. Depending on the type of the originating transaction, there may be multiple second level transactions that are required in order to perform the full and complete movement of funds. In addition, since all secondary level transactions within the system are one way, an originating transaction that requires funds to be withdrawn from one account and

5   deposited into another will inherently require two transactions for this to occur. In addition, the type of accounts involved also affect the total number of secondary transactions that are involved. There may also be additional secondary transactions created in order to account for related actions, such as in the case of Fees or Commissions being attached at the transaction level. This second level is divided into two types, those that are considered "internal" and those

10   that are considered "external".

Internal Transactions are those transactions that transfer funds between accounts that are completely within the domain and control of the Smarte System™ itself. For example, transactions that move funds from one Administration account to another are considered to be internal transactions.

15   External Transactions are those transactions that access accounts that are NOT within the full control of the Smarte System™, such as regular Checking and Savings Accounts, Credit Card Accounts, etc. External Transactions are typically either handled through a transaction portal, such as in the case of a credit card payment, or through the ACH or ATM network. Since both ATM and credit card transactions are "real time", there is no additional level structure

20   maintained for them.

Multiple Transactions may be required within the system based on, but not limited to, the following:

-    Multiple (Split) Payment occurrences within a single Order (Smarte Pay™)

25   -   Payment Transfer from MoveMoney™ based on Commissions, outstanding Balances Owed

-    Activation of Smarte Credit™

140

- Buyer Initiates Transfer of Funds against another Account (Their Own)

- Buyer Initiates Transfer of Funds against another Account (Other Buyer's)

- "Hard" Adjustment to Account Balance

- Required Movement of money between Accounts within the system

5 - Transaction Generation Based on Returns (ACH)

ACH Transactions are processed at regular intervals, and are therefore contained in Batches. These batches are representative of ACH transactions that have been processed to the Federal Reserve via the partner ODFI in accordance with current NACHA regulations and bylaws.

10 Batches are always split/maintained at the individual Product Class level, allowing ease of maintaining the system in regards to returns, reserves, and payment/reimbursement requirements to be maintained without having to add an additional "batch layer" structure to the system. Note that in processing to the Federal Reserve, a single processing "file" may contain multiple Batches, and each Batch must retain reference to which individual "Fed File" it was 15 inserted into.

Transaction Initiation can occur via seven (7) basic actions within the Smarte System™. Note that this does not include Fees and Commissions, as they are generated based on the event level of the originating actions, and is dependant upon the entities involved. FIG. 46 shows the flow for transactions to be generated within the System.

20 All Transactions within the system will follow the following Basic Flow Requirements (based on prior Validation Acceptance for Transaction(s) to occur):

- Determine Percentage "Splits"/Factors as applicable

- Determine Applicable Fees [Order Level]

- Determine Applicable Commissions [Order Level]

25 - Determination of Transaction Requirements (Based on Process Initiation type/Processing Requirements)

- For EACH Required Transaction, the following then applies

141

o Determine Applicable Fees [Transaction Level]

o Determine Applicable Commissions [Transaction Level]

o Create Transaction Record [Internal]

o Create Transaction Record(s) [External] as/if applicable

o Process Internal Transactions

o Process/Batch External Transaction(s)

o Update User Activity Logs – Calculate for Abnormal Activity

o Log Transaction (Activity Logging Detail to be determined upon completion of Transaction Handling)

o Determine and process notifications for Each "Processed" (not batched) transaction (Internal/external)

o For Batch Processing

■ Process Batched External Transactions as required

■ Determine and process notifications for Each "Processed" transaction (Internal/external) within the applicable Batch.

■ Determine and process notifications for Each "Processed" Batch

The flow for the determination of Fees and Commissions from the Order level is displayed in FIG. 47. Details regarding the calculation of Fees and Commissions are described in detail later in this document.

The process for the determination of what specific "second" level transactions are required is detailed in FIG. 48. Note that this does NOT include the additional Fee and Commission generated transactions, as they are dependant upon the combination of all factors and entities involved.

The process for a Buyer Initiated Transfer is detailed in FIG. 50.

Return Processing is a part of the ACH process, however there are more types of returns other than "charge-backs". Returns other than charge-backs occur primarily due to the very

142

nature of the ACH system itself. There are no "confirmations" of transactions that complete successfully, as well as no real-time validation of account information or fund levels within the account. Return Processing must be handled effectively in order to properly manage ACH transactions in their entirety, as well as properly maintain fees charged to Sellers, as well as revocation of Commissions paid to Financial Institutions and Buyers (in the form of reward points). The Processing house that receives the Fed Ready File from MoveMoney™ will also supply (daily if applicable) a "Return" file from the Federal Reserve. This file contains a mixture of all transactions that are returned from the previous batching session at the Federal Reserve against the Smarte System™. Note that there ARE some RETURNS which must be available for DENIAL of RETURN. For example, it is possible that a "Misrouted" return would have been received, in which case the Return system must be capable of producing this. The processing flow for the handling of Returns by MoveMoney™ personnel is as shown in FIG. 51. The Specific Flows associated with the handling of specific types of returns are as shown in FIG. 52, FIG. 53, FIG. 54, FIG. 55, and FIG. 56. A difficulty in the Return System in lieu of the ACH process in regards to Returns bearing the Return Code "R03" requires special handling. These returns are an "offshoot" of the R03 coded returns (Invalid RTN). The handling of these returns in the Smarte System™ is a result of the integration of the Smarte ACHieve™ System. There are three current basic reasons for this type of return. The first is obvious. An invalid RTN was entered in a manner that it passed the "check digit" routine which, based on the guardians within the ACHieve System, would make this type of return extremely rare. The second, which would be more common, is that the Financial Institution maintains SEPARATE RTN's, one for "standard" processing, and the second for ACH ONLY. The Smarte ACH™ engine handle this type "up front", substituting the ACH RTN where it is known.

Unfortunately there is another type of R03 return that is becoming far too common. This occurs when the RTN is taken from, for example, a Buyer's check. The RTN printed on it passes the RTN digit check, and the "Bank" is created in the Smarte System™. What the Smarte System™ can NOT determine is that this RTN is NOT RECOGNIZED by the Federal Reserve.

143

Certain banks/Credit Unions create their OWN RTN account number based on a formula. These formulas are NOT consistent, and vary from Financial Institution to Financial Institution. This occurs largely because NACHA, while setting the standards and rules for the industry, is a Private organization and has NO enforcement authority, except within it's own membership as a condition of membership. One example of how this can occur is when a larger bank buys out a smaller bank. Instead of changing the RTN or the smaller bank, as the FED "deactivates" this RTN, the larger bank continues to process under the smaller bank's RTN. This RTN is therefore valid in structure, format, and is the RTN that is on the Buyer's "Check", but is NOT recognized by the Federal Reserve as valid. Another mechanism is where the RTN is a CALCULATED value, which occurs primarily with Credit Unions (to date). In this instance, the RTN used can actually vary from ACCOUNT TO ACCOUNT for the SAME Financial Institution. Currently only way found to determine this is from history of received R03 coded returns, and identifying not only that the RTN is a "calculated" RTN (in order to PREVENT returns), but to identify them and record them after they have been returned. As a return is received that is coded as R03, there needs to be an additional "validation" that the user is to perform. It IS possible that the RTN (and subsequent BANK was entered INCORRECTLY. In this case, there needs to be BANK RTN Correction Mechanism given to the user. This is the ONLY area that the RTN for a Bank would be permitted to be changed once the bank has been entered. This change would also have to be recursive through all applicable fields and affected records. Note that CURRENT Transactions would NOT be changed, as they must REMAIN as sent, until such time as they can pass through the Return system. Following this correction, the system should prompt the user to RESUBMIT the Transaction using the CORRECTED RTN. This type of CORRECTION record would NOT be added to the NEGATIVE Information Database, as it in no way reflects upon the actions of the BUYER. If the RTN is determined to be VALID by all available means, then the RM Site Managers attempt to validate the mechanism for which the RTN is calculated with the offending Financial Institution. If the Financial Institution relays that they are utilizing a SEPARATE "fixed" RTN for ACH transactions, then a mechanism to ADD this to the Bank's

144

profile must be given to the user. As with the first type, this type of R03 Failure would allow the user to resubmit the transaction, and would NOT be added to the Negative Information Database. However, this RTN would be added to the R03 RTN data file. If it is determined that the RTN is not a FIXED alternate, but a CALCULATED RTN, then the following applies: Two data tables

5   are maintained for this by the System. These data tables contain the following information:

-    Table I contains information for ALL "problem" or revised RTN's based on Returns. Note that is "FIXED" replacement type, this information is ALSO added directly to the Bank Master Record as an ACH Specific RTN.

TABLE I

10   MMC Indent [Bank] (Indexed)

Original (rejected) RTN (Indexed)

Corrected RTN (Indexed)

Correction Mode – Whether "F" – Fixed Alternate or

"C" – Calculated (variable)

15   -   Table II contain records ONLY for those RTN's whose those formulas were added by the Administration USER.

TABLE II

MMC Indent [Bank] (Indexed)

Bank ACTUAL RTN (Indexed)

20   RTN Calculation Formula

Since the ninth digit of the RTN is ALWAYS a check digit, it will always be calculated based on the first eight digits. Therefore, it is NOT included in the retained formula. Formulas are always 24 characters in Length, with every third position (fixed) representing one digit of the first eight digits of the RTN. The convention for the formula is as follows:

25   R   Indicates that this position of the Calculated RTN is taken from the indicated position of the Base, or Parent RTN of the Financial Institution.

A   Indicates that this position of the Calculated RTN is taken from the

145

indicated position of the INDIVIDUAL ACCOUNT of the Buyer.

C   Indicates that this position of the Calculated RTN is ALWAYS the indicated digit (constant) .

?   Indicates that this number is determined by some internal formula, such as a sequential series on the part of the Financial Institution and can not be captured or maintained by the Smarte System[TM], or is UNKNOWN/UNDETERMINED.

The formula, as previously stated, is a fixed length (24 characters) text string, with each physical group of three characters representing the physical position of the calculated RTN.

RTN Digit Position	Formula Position
1	1 - 3
2	4 - 6
1	7 – 9
1	10 – 12
1	13 – 15
1	16 – 18
1	19 – 21
1	22 - 24

Example of Formula String: R1 R2 R3 A5 A6 C4 ? ?

From the example, we can run a pattern check on the first 6 characters of an RTN based on a given return. On a Smarte R03[TM] ISS (Intelligent Sub System) Pattern check, the entire "Problem" data set is retrieved (Table II), and the records are polled individually through the entire set, one at a time. For each polled record, The Returned/Bad RTN is adjusted, based on the formula for the individual RETRIEVED RTN formula. Taking the RETURNED/BAD RTN and Buyer Account Number, use the retrieved formula to calculate a value from BOTH RTNS using the RETURNED ACCOUNT#, using ONLY 'R", "A", and "C" coded values, and inserting the "?" character in the indicated positions by the formula. This results in 2 separate 8

146

digit variables. If the variables match, this RTN is added to a separate list for the user to Select from/Verify ACTUAL Bank. The user MUST be given the opportunity to VERIFY the Alternative Financial Institution. Since there are little or no controls on these formulas, it is entirely likely that two or more Financial Institutions may have MATCHING formulas! In

5   addition to the formula check, there is an additional "Bank Name/Address Search that, if "turned on" by the user, attempts to match a newly added bank with existing records based on name (depth of characters in search to be optionally selected by the user) and any address/phone number information given. This helps to identify "problem" RTN's PRIOR to the record processing and becoming a RETURN. The flow for the "Check" portion of the Smarte R03^{TM}

10   System is shown in the FIG. 57. There is no way that the system could accurately "guess" the individual formulas used by the Financial Institutions. Therefore, they must be determined and manually entered by the individual MoveMoney^{TM} system administration users. The first step is to indicate that a formula is to be entered. This is an additional Option to be given to the User from BOTH the Financial Institution Profile Screen, as well as the R03 Returns Manual

15   Processing Screen.

The user should NOT be required to "KNOW" or understand the formula. The user should be presented with a screen similar to the ones displayed in FIG. 59 through 67. THE SCREENS DEPICTED IN FIG. 59 THROUGH FIG. 67 ARE INTENDED TO BE USED AS A REFERENCE TO THE USER INTERFACE REQUIREMENTS ONLY. THESE ARE NOT

20   THE ACTUAL SCREENS TO BE USED IN THE SMARTE SYSTEM^{TM}. THEY ARE GIVEN AS REFERENCE FROM THE WORKING SCREENS IN ORDER TO PROVIDE A BASIS FOR REQUIREMENTS. After the Search has been completed, a screen similar to the one displayed in FIG. 59 will be shown. A Screen similar to this one would also allow the user to directly enter formulas against a selected RTN. This command option should NOT be added to

25   the "Menu" of the Smarte System^{TM}, but remain as an indirect entry under either R03 Return Processing. In this instance, once a Financial Institution has been selected from the list, an additional option would appear on the screen, similar to as shown in FIG. 60. This gives the user

147

the two options for re-defining an RTN. The first is referred to as a "standard" replacement, as it is always a 1:1 relationship. At this point, the user selects one of the two available options, or selects "cancel". Once an option has been selected, the command which drives the next operation appears on the screen. As shown in FIG. 61, the text on the command (caption) will reflect the option selected by the user. If the user chooses to define a Calculated RTN, the screen as shown in FIG. 62 would be displayed. This is the beginning screen for all RTN formula Calculations. From this point, the user selects which position is to be defined. If the user is retrieving a previously defined RTN (redefining), then the labels to the right will reflect the stored formula as follows:

R: Defined as Position {Stored Value} of the Parent RTN

A: Defined as Position {Stored Value} of the Individual's Account#

C: Defined as a Constant Value: {Stored Value}

?:   Unknown/Not Defined

This series will also appear on the screen next to the applicable RTN position as the individual position definitions are saved. Note that "?" is the default for all positions of the RTN in a NEW definition. Once the user has selected the position to define, the screen would change to appear as shown in FIG. 63. The User then would select the "Define/Redefine Position" command in order to define the selected position. When this is done, the user would be presented with a screen similar to that shown in FIG. 64. Note the option "Unknown or F/I internal Calculation is NOT visible unless the user is redefining a previously defined position. This is only used to "clear" an existing positional definition. At this point the user selects the definition for the selected RTN position. If the definition is "Unknown", then the screen would reflect as displayed in FIG. 66. If the definition is any definition other than "Unknown", the screen would appear as shown in FIG. 67. The text box ("Enter Defining Value" field) is locked to ONLY NUMERIC values, and the maximum allowable length for an entry for the text box is to be adjusted during run-time as follows:

Type "R" or "C": 1

148

Type "A": 2

If type "A", the value can not exceed the length of the specified Account Number

(if entering indirectly against a Return where the Account Number is known)

For ACH Transactions to exist within the system, the following conditions must be met:

5   -   Must be attached to an Order or Administrative transfer of funds.

    -     Must Verify that Transaction would not be "Blocked"

    -     All Information Requirements as specified under the Seller and Product Class

apply.

The transaction itself is generated by the Smarte System^{TM} in response to either an Order

10 generated by a Buyer or an administrative transfer of funds is initiated by MoveMoney. In most cases, the release of the transaction to process should be immediate, however the Seller may place a delay on the transaction as part of their standard processing. In this case, the transaction will be created in the system, but not processed until the release date. This also gives the Seller time to "cancel" the order if any items are returned by the Buyer. Once the transaction is

15 released, the Smarte System^{TM} calculates any Fees to be charged to the Seller and records them. The Smarte System^{TM} also calculates any amounts to be added to the individual Product Class reserves as well. In addition, any commissions are calculated, as well as any Reward Points for the Order are added to the Buyer's profile. If the Buyer has used an account with a pre-authorized limit, the amount of the ACCOUNT used is deducted from the available amount and

20 added to the temporary "holding" reserve for that account. This amount is released at a later time. Once the transaction has been released and available to process, it is "batched" and a Fed Ready file is created. This process is activated manually by MoveMoney^{TM} administrative personnel at predetermined times. The Fed Ready file is then transmitted to the Processing House which in turn transmit it to the Federal Reserve. Once this has been accomplished, any

25 required notifications are also performed. The basic flow for this process is displayed in FIG. 58.

SYSTEM SECURITY, POLICIES, AND PROGRAMMING GUIDELINES

The MoveMoney™ Corporate Security Policy is a high-level document that states senior management's directives for the corporation's overall security.

Digital certificates and Tokens are used for user authentication. Digital certificates and secret key encryption are used for process authentication.

5 - Authentication, authorization, access control framework products provides more security than basic operating system capabilities.

- Security policies ensures that MoveMoney™ defines overall security responsibilities and defines consistent guidelines for performing security-relevant functions.

10 - Encryption provides both data confidentiality and data integrity.

- MoveMoney™ will not be able to control the Seller's web site that the Smarte VII™ platform will be installed in. Thus, some of MoveMoney™ components operate in a "hostile" environment. MoveMoney™ applies least privilege concepts to restrict the capabilities of these components, as well as limit the sensitive information these components can access. The corporate security policy covers these areas:

Issue statement: The policy's goal, the definition of the issue. The primary goals are to maintain high integrity, to prevent fraud and to prevent unauthorized disclosure.

Position statement: Management's decision on how the issue is approached.

20 Applicability: Where, when, how, to whom, and to what the policy applies. Applicability specifies the facilities, hardware, software, information, and personnel that the policy covers.

Roles and responsibilities: The management and technical roles to implement the policy and to insure the policy's continuity. This also outlines the organizational responsibility for operational security and defines employee accountability.

25 Compliance: The policy's definition of how violations are handled and disciplinary actions, such as penalties. Monitoring responsibilities are covered in the responsibilities statement.

150

Legal requirements. The legal requirements for e-commerce services are different in different jurisdictions. Growing concerns over Internet privacy are spurring new legislation and guidelines in this area.

MoveMoney™ supplements the overall corporate policy with detailed operational policies. These provide specific security rules for particular systems, such as the rules and practices that regulate how a system manages, protects, and distributes sensitive information. Examples of operational policies include policies for physical security, platform hardening, disaster recovery, and Internet usage.

The following Basic Programming and Security Implementation Guidelines will be adopted in the implementation of the Smarte™ system. The guidelines address the most common web pitfalls that may leave web applications open to intruder attacks.

Physical Security and Security Awareness are of extremely high importance. Intruders who can gain physical access to systems can plant tools that they can use to gain remote access to the system later, even through firewalls. Other intruders may do physical damage to systems.

Physical security concerns how access to development and production systems is restricted. Another physical security concern is access to non-production systems that have connectivity to production systems. MoveMoney™ will address the following issues in this area: MoveMoney™ will enforce physical access restrictions to the production systems. Servers that contain sensitive information, such as financial account data, will have additional protection.

Security awareness training, including common social engineering techniques, are provided to highlight the common techniques intruders use to gain physical access. It will also make employees cognizant of the need to protect corporate intellectual property from exposure in public conversations and in email.

In the hostile Internet environment, all MoveMoney™ applications are built defensively to be able to withstand intruder attacks. In particular, applications will not trust any input from external sources, including web form entries, hidden field values, applet inputs, or any other data received from an external source.

151

Nothing received from the user, including form elements and hidden fields, are considered trusted. "Bad" characters such as shell escapes and control characters in all user input are filtered. Tainted-Perl concept (any data that comes from an unsecured source is tainted until it's explicitly cleansed of potentially harmful content) to user inputs are applied.

5   Buffer overflows are kept at a watch; Size restrictions to all user inputs are applied.

All incorrect data types (characters in numeric fields, invalid dates, out of range data) in all entries are kept at a watch.

Session ID's are kept long, e.g. 30 characters or more; be random and not repeat over time; not contain any user information, but are tied server-side to a specific user ID; expire

10   within a reasonable time period (e.g., minutes, not days); and be sent over a secure path. The system tracks the user's IP address to avoid IP hopping (changing the session IP address during a session), a probable indicator of session hijacking. In addition, the same User ID will not have multiple sessions at any given point of time.

Temporary files are avoided, and are automatically deleted as they can provide sensitive

15   information to others if file system permissions permit access or if the system is hacked. Moreover temporary files occupy disk space and hence are automatically deleted from the system. Writing of temporary files to publicly accessible directories, such as /tmp are avoided.

User sign-off functions actually sign off a user. Session data are not cached on the user's system. Log out pages are not cached to prevent another user to use the browser back key to

20   view session data. Session timeouts are auto programmed. Users are instructed to close their browser if cookies or other session information may persist. This is done by "in your face" mechanism such as a browser pop up.

Strong ciphers are used to protect information. Web servers are set to require specific ciphers, not negotiate a common cipher set. Otherwise, user could set their browser use no

25   ciphers or message authentication codes, leaving the connection vulnerable to eavesdropping.

Key length may have an impact on application performance. Applications are tested with different key lengths to understand the application impact.

Pages that contain sensitive information for caching are checked. HTTP Headers "no-cache" and "expires" are used to prevent caching.

Anything downloaded to the user could be dissected, altered, and attacked, and therefore the following are recognized and addressed by the system in the design and function: User-friendly variable names are vulnerable to guessing and spoofing; Hidden fields can be edited; Applets can be reverse engineered; Anything in the browser page cache directory are examined; Cookies are analyzed; Minimum amount of data on the user system are cached.

Partial session attacks are avoided. Session resources are not allocated until after the user has successfully authenticated. Otherwise, partial authentication attempts floods could exhaust server resources. Explicit session connection timeouts are set.

Storing sensitive information in clear-text are avoided on externally accessible systems. Sensitive information such as, User Ids and passwords, Encryption Keys, Transaction Data, Credit card numbers, Account numbers, Internal system names and IP addresses and internal user account ID's are especially avoided to be left in clear-text.

Browser-side checks are not reliable. JavaScript, VB Script, or other scripting checks done in the user browser can be easily circumvented. These checks are considered a convenience to the user. All checks are duplicated on the server.

System Hardening. Internet accessible systems are hardened to remove potential vulnerabilities that an intruder could exploit. Services that are not needed to support the application, but that could provide an entrance point into the system would be disabled. Known security holes in operating systems and applications that have not been closed are removed.

Hardened Server Platform. All unnecessary services from the operating system are removed. Extraneous services that may be packaged with the web service (e.g., FTP, file upload, Gopher) are disabled. All unused user ID's are removed. Password rules, especially for administrator accounts are enforced. Strong authentication for administrator accounts, especially for externally accessible systems are applied. Contents in the web server's environment are made known and PATH settings are kept as minimal as possible and absolute paths are maintained.

153

Security patches are kept up to date; system settings are rechecked after patching. Web server admin function are shut down when not in use. Admin functions that are HTML-based, are not externally accessible.

The supporting services that underlie application services are also hardened, and therefore operate securely as otherwise they could be used to provide information for attacks, or as attack launching points. These services are also hardened against Internet intruders. MoveMoney^{TM}'s service provider maintains awareness of current Internet attacks and provides basic services such as IP address spoofing filtering and attack monitoring. (IP address spoofing is where a hacker discovers an IP address assigned to an internal MoveMoney^{TM} host and uses it in traffic that they send from the Internet.) The service provider service contract defines their responsibilities for alerting MoveMoney^{TM} if the provider detects an abnormally large amount of traffic going to MoveMoney^{TM}'s site.

MoveMoney^{TM} will review its service agreement to ensure that it contains provisions for basic security services. The agreement will clearly state the service provider's responsibility and time windows for notifying MoveMoney^{TM} of suspicious Internet activity.

IP-based access restrictions. IP address restrictions is used in conjunction with a DNS reverse lookup. This check verifies that the IP address is registered in a valid DNS map, and that the DNS map has matching entries for IP-hostname and hostname-IP. This helps prevent IP spoofing attacks. The following restricts the IP addresses that can connect to a particular service: Service user ID and file system permissions: If the web server is broken into, the intruder will most likely gain access to the user ID that the web service runs as, either by gaining access to a shell or by tricking the application into running arbitrary commands. The user ID has as few privileges as possible. For example, the user ID will not be able to replace any of the application class files or executables. File system permissions applied to web page and other application files, such as servlets, JSPs, ASP, CGI executables are also checked.

Directly accessible content on all systems involved in the application, especially externally accessible systems are outlined. Directly accessible ports on every system are

154

outlined. Directories indexed for search are outlined. Directories containing restricted files or sensitive information are not indexed. Directories are not browsable, especially directories containing sensitive information, configuration files, or application executables. Security configuration recommendations for customers to warn them about potential risks are developed.

5 The following are a part of the system: User browser option settings, such as disabling caching encrypted pages to disk; file system permissions settings for unmasks and application file system permissions; platform hardening; required Service account privileges; and environment settings needed for the application.

MoveMoney™'s production systems is tightly controlled, both for security and stability

10 via a Secure Administration. MoveMoney™ administers its production systems itself. Since the production systems is housed at a remote facility, MoveMoney™ uses a secured communications line to provide a secure communications path from its development office and the production site. Secure administration approach includes:

Monitoring: Event notices transmitted over un-secure media can be viewed, altered, or lost.

15 Event notices can potentially give outsiders information on the type and configuration of the internal system components.

Remote administration is done with extreme care and limited to only a small specific group of individual user computers, as otherwise it can introduce security holes by transmitting privileged user authentication information over a network where it may be monitored and

20 recorded. In addition, privileged commands may also be transmitted in the clear, where they can be recorded and replayed. Administrators have not left any backdoors in remote systems to facilitate remote access.

Security criteria is included in the administration tool selection criteria. Features that strengthen the tool's security include support for strong authentication and replay attack

25 prevention features.

Security principles define the fundamental security concepts for the system. The MoveMoney™ system has these principles:

155

- Resource privileges to subjects. These privileges are the ability to create, modify, and delete resource instances, and to read and write resource attribute values.

- Subjects have full privileges to the resources they create.

Example: a financial institution user creates a buyer account. The financial institution user can view and change the buyer's account information, or can delete the account.

Subjects can authorize other subjects to have access to the subject's resources.

Example: the financial institution can grant a buyer 'read access' to all of their (the buyer's) information. The financial institution can grant a buyer the ability to create specific new information within their (the buyer's) account, such as address book entries, and to modify other data, such as the default shipping method. The financial institution retains the right to view any of the buyer's data, such as for customer service.

- Subjects can create subordinate subjects.

Example - buyers may create sub-buyers who may access the buyer's account.

Subjects can control the authorizations of their subordinate subjects.

Example - a buyer may authorize a sub-buyer to only be able to view transaction histories. The sub-buyer cannot create new transactions.

The main Application Security Components for the MoveMoney^{TM} distributed applications are as follows:

- Authentication component assure a subject's identity, that is, the subject is in fact who it claims to be.

- Authorization and access control component assign privileges to subjects and control subjects' access to resources based on those privileges.

- Accountability component uniquely traces a subject's actions to it.

- Data integrity component assures data is not altered without authorization.

- Confidentiality component assures data is not disclosed without authorization.

156

MoveMoney™ requires subjects to pass Authentication at system entry points, i.e., the external service perimeters and internal system boundaries. At each point, MoveMoney™ requires one-way or mutual authentication. External entry points are accessible from the Internet. The entry points are:

5   -   MoveMoney™ web server: End users authenticate before they will be allowed to manage their MoveMoney™ profile via the MoveMoney™ web application.

    -    MoveMoney™ payment server:

        o Buyers are authenticated before they will be allowed to access their MoveMoney™ account for payment. This authentication is passed through

10   the seller's web application to the payment server via the Smarte VII™ platform.

        o Seller systems authenticate to the MoveMoney™ payment system before they can submit transactions.

Internal service points will be accessible to internal MoveMoney™ systems and users. The entry

15 points are:

    -    Admin server: Administrators are authenticated before they are allowed access to MoveMoney™ administrative applications.

    -    Application server: Depending on the security of the internal LAN, direct access to the application server requires authentication.

20 -   Remote access: The remote access server acts as a gateway between a remote MoveMoney™ location and the MoveMoney™ systems at the service provider facility so that MoveMoney™ employees can administer the operational MoveMoney™ systems. The remote access device may be a separate device, may be integrated with the service provider firewall, or may not be used if the

25   communications link is a private leased line.

    -    Database server: The database server requires authentication to access the MoveMoney™ database.

157

The MoveMoney™ system uses two main categories of authentication: User (human) authentication and Process authentication for inter-process interactions. User authentication prompts the user to enter authentication information. With process authentication, the process invokes the authentication mechanism automatically. Since the Smarte™ suite of offerings deals with payment and financial institution accounts, MoveMoney™ uses very strong authentication mechanisms. Most credit card services do not use strong authentication, so this provides MoveMoney™ increased security over most credit card services.

Challenge/response: The system produces an unpredictable challenge that varies with time. The subject generates a response, using secret information known only to that subject. MoveMoney™ adopts the challenge/response based on digital signatures and public key certificates. With this type of challenge/response system, the subject is given some data that it must digitally sign to prove its identity. The recipient of the signed challenge verify the signature with the subject's public key. Digital signatures are based on RSA algorithms, the most prevalent in the industry today. The subject being authenticated has public key/private key pair and public key certificate. For others to accept the subject's public key certificate as genuine, the certificate is issued by a trusted third-party. The subject's private key is protected, as it constitutes the actual proof of the subject's identity. Secure Sockets Layer (SSL) uses this form of challenge/response authentication. Smart cards or Custom CDs are used to store the private key and certificate. The card or CD can perform the cryptographic functions so that the private key is never exposed. Smart cards require the subject to have a smart card reader and Custom CDs require the subject to have a CD ROM drive. Key pairs can be generated by browsers and stored in the browser's key database, but this renders them susceptible to theft. Key pairs for special use uses RSA's BSAFE Crypto-C cryptographic libraries. Certificate generation is done with RSA's KEON Certificate Server using the RSA's BSAFE Crypto-C cryptographic libraries.

Token: A token is something that a subject possesses that they present as part of their authentication. MoveMoney™ will use RSA SecurID for the Token authentication. This is a physical or software device that displays a time-varying multi-digit number (the number changes

158

once a minute). To authenticate, the subject must present their user ID, the current number, plus the PIN they get assigned when they signup.

Another important facet of an authentication component in the MoveMoney™ system is how failed authentication is handled. The failure handling will not reveal any additional information about the subject or why the authentication failed (e.g., an error message will state "authentication failed" not "invalid password" or "invalid user ID"). Limiting the number of authentication retries prevents guessing attacks. Repeated login failures generates a security event to detect systematic attacks. MoveMoney™ logs these events. The system also supports sending notices to the owner of the account experiencing the failed logins. Authentication state tracking is an important part of session management for web applications. The web application distinguishes each authentication phase so that subjects cannot bypass authentication.

Authorization consists of granting one or more privileges to a subject. MoveMoney™ Authorization mechanisms assigns privileges at different granularities. For financial systems, granular privilege assignments are required. Since financial account data is highly sensitive, MoveMoney™ assigns permissions for viewing, modifying, and deleting to specific resources. Furthermore, the authorization system supports the ability for subjects to allocate some or all of their privileges to other subjects, but constrains the allocation so that subjects cannot give away privileges they do not have.

In the MoveMoney™ system, authorization takes place as follows:

-    When a new user account is created or modified. The creating subject assigns privileges to the new subject so that the new subject can access its MoveMoney™ profile and its MoveMoney™ funds.

-    By explicit action of superior account. For example, a user can explicitly grant privileges to a sub-user.

-    By delegation: In delegation, a subject authorizes another subject to act on its behalf, with some or all the original subject's privileges. For example, a process will assume a user's identity and perform actions on the user's behalf.

159

The authorization database and authorization assignment functions will be secure or subjects will be able to adjust authorization assignments themselves.

Access Control mechanisms enforce the permissions a subject must have to access resources. Access control can be controlled with widely differing granularity, ranging from no access controls to controls on individual resources within applications, such as fields within database records. As with authorization mechanisms, MoveMoney™ requires access controls with the ability to support a wide range of granularity, in particular, it enforces that subject's have the required permissions before granting access to sensitive resources. Access controls thus applies to all subject types, human and machine. MoveMoney™ employs the following access controls:

- Operating systems: Intrinsic permission enforcement controls that are built into the operating system. The operating system enforces owner/group/public permissions for read/write/execute.

- Policy objects: An object-oriented approach to access control, where a policy object defines the attributes needed to access a resource. Subjects are assigned privilege attributes; the policy object maps authorization privileges to access rights.

- Container-based: A container provides an execution environment for entities that reside within in it. Part of this environment is access control based on the container's security policy.

- Access control lists: A permission list associated with a resource that defines the privileges a subject must possess in order to gain access to the resource and the type of access the subject is permitted.

- Rules: Rules define a set of characteristics or conditions that must be met before access is granted.

160

- Labels: Mandatory access control is based on sensitivity labels assigned to resources. Subjects must be cleared to access the sensitivity level defined in the label before being allowed access to the resource.

- Capability-based: A capability identifies an object and a set of access rights to that object. Any subject that holds the capability can use it to perform the operations permitted by those rights. Capability-based security is efficient because no special checks are needed to verify that a subject has a particular permission; the possession of the capability signifies that permission has been rightfully obtained.

Internal access points occur whenever a subject or process accesses a resource. Access controls are applied whenever a subject requests access to a resource. Caching permissions can improve performance, as can dynamically adjusting the function set made available to a subject so that the subject only "sees" permitted functions. For example, a user's GUI is dynamically constructed so that the user only sees the menu items they are authorized for, reducing the access control checking needed in the GUI. Web applications need to pay particular concern to access controls, since some users will attempt to subvert access controls wherever possible. Issues that are considered include:

- Menu bypass. If users can gain information on how menu items are invoked, they may try to bypass the menu system and invoke functions directly. The menu system does provide information on how internal functions are accessed.

- Direct invocations of web resources. As an example, Java servlets can be accessed by directly connecting to their URL. Unless the servlet first applies access controls, this may enable a subject to invoke the servlet's functions without authorization. Implementing access controls in all servlets is highly redundant. Therefore a central servlet dispatcher that performs the access check, then dispatches the correct servlet for the function is implemented for efficiency.

- Interprocess communications.

161

- Direct connections to sockets. Any service that listens for connection on a socket will assume that only authorized subjects will connect to it. The application performs an additional access control check, or network access will be restricted.

- Named pipe, other IPC methods. Any service listening for connections ensures it does not accept unauthorized connections, or the environment is set up to restrict possible connections.

- User session handling. Web applications require some form of user session identification to track and control a user's actions. This session ID is not predictable or guessable. The session ID generator also has a good random number generator. Sessions have a finite lifetime to prevent session theft or hijacking. Session information is sent to the user's browser in three main ways:

  o A cookie. This is stored in the browser-specific cookie store. Since the cookie is in a file, the user must find the cookie file to view the cookie. In addition, the cookie itself is a session value, so no hard file is stored, making it more difficult to capture. In addition, The web application expects that users might tamper with cookies. Integrity checks are applied to help detect tampering.

  o A hidden field. This information is encoded in HTML tags within the form itself. The user can view the session ID by viewing the page source.

  o URL encoding. The session ID is appended to the URL in a particular format. The session ID is visible at all times.

Accountability mechanisms ensure that a subject's actions can be uniquely traced to it. Two accountability mechanisms are applied to the MoveMoney™ architecture: audit logging and non-repudiation.

Audit logs record a permanent trace of a subject's actions. An audit policy defines the security relevant events that are recorded, for example log on, log off, failed authentication, and

162

other events that affect system configurations or sensitive user application data. The policy also defines what actions to take when audit logs reach their maximum size.

All audit log records are sent to a central audit facility. The audit event notices adhere to a standard format. An event notification protocol transmits the event notice from the emitter to the central collection system. RSA Security Keon Event Logging Server's advanced PKI products and Emails route event-logging information to a centralized Event Logging Server (ELS) against which reports may be run. Monitoring products filter log records for patterns of events that indicate potential security incidents. Some products automatically generate alerts to administrators. Administrators can thus receive one meaningful notice as opposed to many low level events. Secondary event notices are generated as a result of an event or a combination of events. For example, the MoveMoney™ system logs failed authentication attempts, but also forwards an event notice to the account holder and to administrators in the case of repeat authentication failures. The audit records are archived for a period long enough to support potential investigations. In addition, the records are protected against change in case a dispute or security incident needs to be investigated. Periodic audit reports are generated as a useful management tool since they show usage patterns.

Non-repudiation mechanisms provide proof that a subject participated in an action. The exact nature of the proof required vary according to the laws in the jurisdiction. Proofs that may be required include proof that the sender intended to perform the action (e.g., buy something), proof that the transaction actually came from the sender, proof that the transaction has not been altered since the sender initiated it, proof that the communication between the two parties occurred, and proof that the transaction record has not been altered. Non-repudiation is a complex subject, since the legal requirements for evidence are not the same in all jurisdictions. In the United States, non-repudiation is tied to digital signature legislation. Currently, the States are enacting their own legislation, as is the Federal government. The situation overseas is about the same. Technology to support non-repudiation is still "leading edge". Few, if any, non-repudiation lawsuits have taken place. When they do, the legal requirements will become

163

clearer. In the near-term, mechanisms that will support non-repudiation in the MoveMoney system include:

- Application-level signatures on submitted form data. eXtensible Markup Language (XML) is used as the preferred method of structuring signed forms.

5 - Signature verification. For a digital signature to have meaning, the application establishes that the user's certificate was valid at the time of the action. This verification requires verifying the digital signature on the certificate, checking the certificate's validation period, and checking the certificate against the issuing certificate authority's Certificate Revocation List (CRL).

10 - User intent. Most jurisdictions' rules of evidence require some indication of the user's intent to sign the transaction. This helps to establish that the user is fully aware of the consequences of their signature.

- Time-stamps. The application applies a timestamp when the signature is applied. Without this, the application cannot check that the certificate was valid at the time 15 the action took place. The timestamp is "secure", i.e., unforgeable.

- Secure audit trails. Records of the non-repudiation action is stored so that they cannot be changed after the action has occurred.

Digital signatures are a primary means of obtaining non-repudiation. Multiple digital signatures may be needed to achieve non-repudiation sufficient for a legal contest.

20 Non-repudiation can occur at multiple levels in the application:

The endpoints in the communication session, such as an SSL session, exchange a secured data structure, such as a digital signature, that authenticates them. This validates that a session between the sender and receiver took place.

Interactions between middleware services, such as between object request brokers 25 (ORBs), include a secured data structure, such as a digital signature, that validates the service's authenticity. Interactions are securely time-stamped and logged. This validates that an interaction took place.

164

The transaction is accompanied with a secured data structure, such as a digital signature, that validates its authenticity; the transaction is time-stamped and logged. This validates that a transaction took place.

The end-user's intent to take the action is recorded, the application actions are uniquely and irrefutably traced to the user by the user digitally signing the transaction data, and the action is securely time-stamped and securely logged. This validates that the user's intent to engage in the action and that the action took place.

Data Integrity mechanisms ensure that data has not been altered or destroyed by unauthorized subjects. Data integrity mechanisms are usually based on hash functions that use a one-way immutable function to produce a unique value from the variable length input data. Simple checksums produce a hash using low-overhead algorithms. Encrypted checksums are simple checksums that have been encrypted using a secret key. An encrypted checksum is harder to alter than a simple checksum. The SSL protocol uses an encrypted checksum called a message authentication code (MAC) to detect changes to data while in transit. Digital signatures combine a hash function and asymmetric encryption to construct a secure encrypted hash of a specific set of data. Data integrity mechanisms apply primarily to data. Data integrity are applied to the sensitive user information, including user and transaction data stored in the MoveMoney™ database.

The main categories of the MoveMoney™ data integrity mechanisms are as follows:

- Encrypted checksums. Encrypted checksums are simple checksums that have been encrypted using a secret key. An encrypted checksum is harder to alter than a simple checksum. A special case of an encrypted checksum is a message authentication code (MAC). MoveMoney™ encrypted checksums are encrypted with RSA asymmetric encryption. Encrypted checksums are typically applied to data where change detection is important. Common uses are audit records of financial transactions where they transaction may later be disputed.

- Message authentication code (MAC). MACs are one-way hashes produced using secret key encryption. MACs are primarily used in communications sessions to verify the data's origin and that the data exchanged was not altered en route. MACs are used to protect communications against undetected change.

5   - SSL: The SSL session's master secret is hashed into a sequence of secure bytes. Part of the secure bytes are used for a MAC secret. The MAC secret is hashed with the message data, then hashed again with the results of the first operation. The output of the MAC operation is encrypted according to the negotiated session cipher specification.

10   - Digital signatures. Digital signatures combine a digest function and asymmetric encryption to construct a secure digital signature of a specific set of data. Specifically, a digital signature is a digest computed over a specific set of data using a message digest algorithm. The computed digest is then encrypted with a private key. The signature is verified by re-computing the digest with the same

15   algorithm over the same data set. The signature is decrypted with associated public key, and the decrypted digest value is compared with the original digest. If the values match, the signature verifies; otherwise verification fails. Where Digital Signatures themselves are utilized, the RSA algorithm will be applied in the MoveMoney^{TM} system.

20   All these data integrity mechanisms are applied as applicable in the MoveMoney^{TM} system. Simple checksums are used in internal environments for change detection. Encrypted checksums and digital signatures are used for protecting transaction data, especially if the transaction data may be disputed. MACs are used with SSL. Data integrity mechanisms have two main issues: where to apply them and how to manage encryption keys when encryption is

25   used. For end-to-end integrity, data integrity mechanisms are applied at the point the data is created and passed through with the data throughout the data's lifetime. Data integrity

166

mechanisms provide change detection, but also incur both processing and storage overhead. Issues for key management include the following:

- Key distribution: Delivering keys to subjects are done electronically through participating Financial Institutions or Exchanges.

5
- Key update: Keys are changed periodically. Updating a key reduces the risk of the key's exposure over time. Key update involves not only key distribution for the new key, but keeping track of when keys are due to expire.

- Key revocation: If a key is exposed, it will be invalidated so that it can no longer be used. This can be as simple as refusing to accept the key, if the key is only

10
used in pair-wise connections. Asymmetric keys would be reissued through the certificate authority. The certificate authority will revoke the public key certificate and include the certificate in the certificate revocation lists that it issues.

- Key backup: Encryption keys will be stored in a secure backup facility. If the

15
keys are lost, the backup copy of the key can be used to replace the lost key.

Confidentiality mechanisms ensure that information is not disclosed to unauthorized subjects. Confidentiality mechanisms are usually based on encryption, where symmetric key algorithms, asymmetric key algorithms, or both, may be used. As with the data integrity service, the confidentiality services also primarily apply to data. Data confidentiality applies to data in

20
transit and data in storage. The main categories of data integrity mechanisms are as follows:

- Symmetric key encryption: All parties authorized for the data will have an access to the decryption key. Symmetric key encryption are applied for pair-wise confidentiality, e.g., only the data owner and the MoveMoney^{TM} system are authorized for the data. If more subjects are authorized, then group encryption

25
keys are needed.

- Public key encryption: For confidentiality, the asymmetric keys are used in the opposite fashion from a digital signature – the subject's public key encrypts the

167

data, then only the holder of the matching private key can decrypt the data. This provides strong individual privacy protection since only the private key holder can access the data.

- Proprietary Encryption: In addition to the standard, additional encryption routines may be utilized for data that is not of a "critical" nature, but should still be afforded some measure of protection.

- Combinations of Encryption Techniques: Where information is of the utmost critical nature, multiple encryption methodologies may be utilized in conjunction with each other.

Privacy legislation may mandate the confidentiality mechanisms that must be used in a jurisdiction. Unfortunately, at this point in time, these legislative efforts are not coordinated and jurisdictions are each developing their own legislation. Thus, privacy regulations vary across the state and federal government in the United States, as well as in Europe.

Confidentiality mechanisms are used for data in transit and in storage. Sensitive information passes through the following stages:

- User browser to the seller web server: The SSL protocol encrypts data in transit between the user browser and the seller's web server with symmetric key encryption. MoveMoney^{TM} minimizes any sensitive information sent to or stored in their components on the seller's web server.

- Seller web server to payment server: The MoveMoney^{TM} payment server is externally accessible. All sensitive information that must be cached on it is protected.

- User browser to MoveMoney^{TM} web server: The MoveMoney^{TM} web server is externally accessible. All sensitive information that must be cached on the MoveMoney^{TM} web server is protected.

- MoveMoney^{TM} web server to application server or database, MoveMoney^{TM} payment server to application server or database: The MoveMoney^{TM} web server

168

and payment server is externally accessible, the application server and database are internal systems. MoveMoney™ works with its service provider to ensure that data passing from externally exposed systems to internal systems is not be externally visible.

5   -   MoveMoney™ application processing: The application server resides in the internal MoveMoney™ environment. Sensitive information that the application server places in persistent storage or cache are protected.

-    MoveMoney™ application to database: This communication occurs over MoveMoney™'s internal LAN.   This environment is adequately secured, communications are either cleartext or encrypted.

10

-    MoveMoney™ database storage: Sensitive information that are stored for a long time are protected against exposure.   This reduces the chance that a MoveMoney™ employee can inadvertently or deliberately access the information. It also makes an intruder's ability to access information harder.

15   -   MoveMoney™ application to ODFI: This will be a private interface. The ODFI has its own interface guidelines; and MoveMoney™ has ensured that their information's security is protected.

The privacy service's use of encryption addresses the issues of Key Management and Certificate Authority.

20   System Failure Handling and Recovery from failures are second-tier security concerns. Failures may or may not be caused by security problems; however, if they are not handled within specific time periods, the effect can be the same as a successful denial of service attack. MoveMoney™ incorporates the following:

-    System failure detection and reporting starts with logging and monitoring. 25   Integrated system and application monitoring includes the DMZ systems and supporting services. The strategy addresses how outages are detected and to whom they are reported.

169

-       Disaster recovery planning covers procedures for a wide ranges of potential outages, from simple system failures to more catastrophic, widespread failures. MoveMoney^{TM} has recovery plans for its applications so that recovery responsibilities are clear and can be tested consistently.

5   -   Internet attack recovery is a special case that will be addressed in the disaster recovery plans. The recovery assigns responsibilities to the service providers and to MoveMoney^{TM}.

CRITICAL/ABNORMAL ACTIVITY CALCULATION AND TRACKING

The Guardians within the Smarte System^{TM} monitor the Buyer's activity to determine abnormal or unusual "behavior" on the part of the Buyer. This is a critical feature in order to help prevent potential fraud. In addition to this function, this information also serves as a way to provide the applicable entity with a quick "statistical" information view regarding activity. The Table depicted in FIG. 68 lists a collection of calculation information fields that are common to the applicable profiles. The referenced fields in the Table in FIG. 68 are attached to each individual Buyer as well as each of the individual Buyer's accounts. This allows the Smarte System^{TM} to monitor abnormal activity not only at the individual account level, but for the individual themselves. In addition, this also allows the Smarte System^{TM} do determine the "preferred" method(s) of payment by a particular Buyer (future addition to the system). All variables from individual accounts are ROLLED UP to the individual Buyer's profile. Sub-Type Buyer information is NOT rolled up to the Parent Buyer Profile or Account, although it is VIEWABLE by the Parent Buyer.

All variables are to be initialized at a value of zero (0), regardless of data type, with the exception of CALCDATE, which is set to current system date

"Running" totals and averages are updated ONLY when the DAY or WEEK changes. If this is NOT done in this manner, then the averages would be skewed in favor of abnormal activity, especially when the user is "new" to the system and the history log is sparse.

170

Prior to beginning any calculations, the current calculated date (CALCDATE) is to be compared to the SYSTEM date. The program maintains variables indicating the following at this point: Same Day? (Y/N) and Same Week? (Y/N). Duplicate Calculations for BOTH Individual Account and in Buyer Profile Records. The Following calculations are valid for BOTH tables! If Buyer has SPLIT the payment across multiple accounts, the term {Trans Amount} is valid ONLY for the amount that is charged against the individual account. In this instance, these calculations must be performed for each individual account for the individual amount charged against them. For the Buyer Profile, the TOTAL AMOUNT of the Transaction is used in the formula where the term {Trans Amount} is referenced. The following formulas DO NOT include any required conversions of data types in

order to perform calculations. Note that data table and field names may very from system to system and are not required to be maintained identical to those specified herein. The calculations occur as follows for the given scenarios:

- Guardian Calculations PRIOR TO "Recalculation"

Prior to Calculation, the current days/weeks activity is re-averaged and compared to the history level averages in lieu of the given trigger points. This is done prior to performing the actual transaction, as this allows the Guardians to intercept abnormal activity PRIOR to the transaction actually taking place.

(((TDTOTENTSBYD + {Trans Amount}) / (TDTOTENTSBY + 1)) / AVGNOFBUYA) * 100

(((TWTOTENTSBYD + {Trans Amount}) / (TWTOTENTSBY + 1)) / AVGNOFWBUYA) *100

The results of these two calculations are then compared against the following Field values IN THE ORDER GIVEN (Most to Least Severe):

DEVDTRGGRS (Suspended – Trans Blocked)

DEVWTRGGRS (Suspended – Trans Blocked)

DEVDTRGGRW (MMC/Bank/Buyer Warned)

171

DEVWTRGGRW (MMC/Bank/Buyer Warned)

DEVDTRGGRB (Buyer Warned – Self Set Limit)

DEVWTRGGRB (Buyer Warned – Self Set Limit)

- Buyer Transaction, Same Day, Same Week

TDTOTENTSBY = TDTOTENTSBY + 1

TWTOTENTSBY = TWTOTENTSBY + 1

TDTOTENTSBY = TDTOTENTSBD + {Trans Amount}

TWTOTENTSBY = TWTOTENTSBD + {Trans Amount}

- Buyer Transaction, New Day, Same Week

AVGNOFBUYS = ((AVGNOFBUYS * TOTBDS) + TDTOTENTSBY) / (TOTBDS + 1)

AVGNOFBUYA = ((AVGNOFBUYA * TOTBDS) + TDTOTENTSBY) / (TOTBDS + 1)

TOTBUYS = TOTBUYS + TDTOTENTSBY

TOTACTBUYS = TOTACTBUYS + TDTOTENTSBYD

TOTBDS = TOTBDS + 1

TDTOTENTSBY = 1

TWTOTENTSBY = TWTOTENTSBY + 1

TDTOTENTSBY = {Trans Amount}

TWTOTENTSBY = TWTOTENTSBD + {Trans Amount}

CALCDATE = {System Date}

- Buyer Transaction, New Day, New Week

AVGNOFBUYS = ((AVGNOFBUYS * TOTBDS) + TDTOTENTSBY) / (TOTBDS + 1)

AVGNOFBUYA = ((AVGNOFBUYA * TOTBDS) + TDTOTENTSBY) / (TOTBDS + 1)

172

$$\text{AVGNOFBUYS} = ((\text{AVGNOFWBUYS} * \text{TOTBWS}) + \text{TDTOTENTSBY}) / (\text{TOTBWS} + 1)$$

$$\text{AVGNOFWBUYA} = ((\text{AVGNOFWBUYA} * \text{TOTBWS}) + \text{TDTOTENTSBY}) / (\text{TOTBWS} + 1)$$

TOTBUYS = TOTBUYS + TDTOTENTSBY

TOTACTBUYS = TOTACTBUYS + TDTOTENTSBYD

TOTBDS = TOTBDS + 1

TOTBWS = TOTBWS + 1

TDTOTENTSBY = 1

TWTOTENTSBY = 1

TDTOTENTSBY = {Trans Amount}

TWTOTENTSBY = {Trans Amount}

CALCDATE = {System Date}

These processes are to be taken care during the processing of an order against both Retail Buyers and Commercial Buyer Users. Note that "retail Buyer" includes Sub-Buyers. Since the structure, formulas, and logic are designed to eliminate the need for a "batch Processing type of calculation, which would be less effective and require more resources to accomplish, it must be retained as dynamic, calculated at the TIME OF THE ORDER as Part of the Order Validations. Without this dynamic calculation, then it becomes a "hindsight" function, rather than "active" guardian within the system. If done on the back end, we would only be "identifying potential fraud", RATHER than Identifying AND preventing it. Therefore we WILL include this as a GUARDIAN in order for the order to process. "Active" refers to what is going on "currently". Since it is likely that a Buyer will perform more than a single order over the calculated periods of time, this serves as a "bucket" to hold the values for the current time periods. Once the individual calculation period is "reset", these values are "zeroed out" after application to the running averages/totals. In addition, there is no "Active Date" within the table, only "active values". These values are maintained individually for each Retail Buyer/Commercial Buyer User within

173

the system. There is no consolidation of this information across different Buyers. This is NOT a Batch Process. It is dynamic and acts as a Guardian as a precursor to Order Validation/Approval as defined.

SMARTE CREDIT™ INTEREST AND LATE FEE CALCULATIONS

5   Interest Calculation occurs specific to the INDIVIDUAL loan activation. Therefore, the system may maintain multiple loan activations with independent interest calculation dates.

Minimum Monthly Payment Amount Due is based on the accumulation of all outstanding loan amounts against a SINGLE Smarte Credit™ ACCOUNT, NOT at the individual activated loan level. The individual requirements, and fees are based on information as supplied by the individual sponsoring Financial Institution at the time the account was created. It is also possible that a Financial Institution may indicate to the system that there is NO late payment fee, or minimum payment amount due.

The Late Fee Calculation function is to be run once per day, and is to be added on to the END of the Smarte Credit™ Interest Calculation routine. It is NOT to be incorporated within the same procedure, but rather is to be maintained as a separate "pass".

The Tables depicting the fields referenced within this section are depicted in FIG. 69, FIG. 70, and FIG 71. Note that data table and field names may very from system to system and are not required to be maintained identical to those specified herein.

The following Default Values are to be entered for the following fields added to Table MMC_ACC_SMARTE_CREDIT FOLLOWING other calculations/entries for the record:

NEXT_PAY_DUE_DATE – Calculated as follows:

If System Date - DateValue({Current Month} & "/" & PAY_DUE_DATE & "/" & {Current Year} <

30 Days then

NEXT_PAY_DUE_DATE =

DateValue({Current Month +1} & "/" & PAY_DUE_DATE & "/" & {Current Year}

174

Else

    NEXT_PAY_DUE_DATE =

    DateValue({Current Month} & "/" & PAY_DUE_DATE & "/" & {Current Year}

5   NEXT_PAYDUE_AMOUNT – Calculated as follows:

Note: calculation assumes requirement for (*0.01) in regards to percentage, but this factor is dependant upon actual method of storage within database.

    If DEF_PER_BAL_DUE * CUR_BAL * 0.01 < MIN_MON_AMT_DUE, then

        NEXT_PAYDUE_AMOUNT = MIN_MON_AMT_DUE

10   Else

        NEXT_PAYDUE_AMOUNT = DEF_PER_BAL_DUE * CUR_BAL * 0.01

LFC_CARRYOVER_BAL – Initial Value

LFC_YEAR – Initial – Current System YEAR

LF_PAID_CUR_YEAR – Initial Value: $0.00

15   LF_PAID_PREV_YEAR – Initial Value: $0.00

The following Default Value is to be used for the specific Field in Table MMC_TRAN_SMARTE_CREDIT_LOAN for Record Generation during Time of Smarte Credit[TM] Account Activation Record Creation: TOT_LFC_CHARGED – Initial Value: $0.00

20   The System flow for the calculation of Late Fees is as shown in FIG 72. Following these calculations, a log record is generated in MMC_SMARTE_CREDIT_LF_LOG.

Calculations following the Smarte Pay[TM] Down Process are as follows:

    Table: MMC_ACC_SMARTE_CREDIT

    If PAY Down Amount > NEXT_PAYDUE_AMOUNT then

25   LFC_CARRYOVER_BAL =

        LFC_CARRYOVER_BAL + Pay Down Amount – NEXT_PAYDUE_AMOUNT

175

NEXT_PAYDUE_AMOUNT = 0

Else

NEXT_PAYDUE_AMOUNT = NEXT_PAYDUE_AMOUNT − Pay
Down Amount

5   The LFC_CARRYOVER_BAL field is used to allow OVERPAYMENT of Minimum
Account Monthly Payments, as is currently done in loan situations. This allows the system to
manage over-payments of minimum amounts by Buyers. It is therefore possible that a Buyer
may, with a single large payment, drive the system to a $0.00 required payment balance for more
than a single month. Since this balance/information is maintained independently of the Interest
10   Calculations, a Buyer can pay a large sum, and therefore not be required to make a payment for a
number of months while still accruing applicable interest on the individual loans.

BATCH PAYMENT CALCULATIONS

          The basis for the payment system is to redirect funds currently maintained within various
entity ADMIN type "holding" accounts to physical accounts maintained by those entities. This
15   includes reimbursement to Sellers for Purchase Amounts (less applicable fees/reserves), as well
as commissions paid to various entities.

          This section concerns flow requirements for "back-end" transaction processing as a result
of any combination of Smarte Cash™, Smarte Credit™, and/or Smarte ACH™ transactions. The
general principles within this section apply to ANY transaction combination not specifically
20   mentioned, or any Future account/transaction type combination added to the system.

          The Payment process follows the following flow:

-          ADMIN PAYMENT PROCESSING Entry Screen.

           o   List of Records in MMC_BATCH_PAY_DUE [Ref: FIG. 73] where Status
               Indicator is NOT the equivalent of "Paid".

25   o   Information to be listed: Entity MMC_ID, BCN (Generated Against) Date
               Due, Amount Due, Holding Account ID to physically Pay against. Column

176

Sorts by: Entity MoveMoney™ ID, Date Due, and MoveMoney™ Holding Account ID.

o Each listed item will have a "Check Box" against which to indicate payment to be processed. A Single Command at the top of the screen will be "Process Payments for Indicated Items."

- ADMIN PAYMENT PROCESSING Confirmation Screen:

o Following Processing, a screen will give the following information:

▪ "Payment Processing Transactions Generated Successfully"

▪ {Total Amount Processed}

There are no Commissions to be applied within the system INDEPENDENT of an ORDER (or subsequent level) event. Therefore, no special "non-order" related BCN handling procedures apply to the Smarte System™ at this time, however, the system IS designed and structured to allow this in the future should the need arise.

The following are System Flow/Calculations regarding Payments:

- At the time of initial Order/Transaction Generation, the system generates the amounts in the MMC_BATCH_PAY [Ref: FIG. 74] as follows:

o System Search for match of combination of BCN and BATCH_ENTITY. If match found, amounts added to BOTH ORG_PAY and ACT_PAY amounts for "both" records as applicable, depending upon information within the MMC_PROD_CLASS_MAS Table [Ref: FIG. 26; FIG. 27].

o If NO record found, record(s) created and amounts added to BOTH ORG_PAY and ACT_PAY amounts for "both" records as applicable, depending upon information within the MMC_PROD_CLASS_MAS Table [Ref: FIG. 26; FIG. 27].

o Determination of single vs. multiple record requirement based on the current information in the following fields in the MMC_PROD_CLASS_MAS Table [Ref: FIG. 26; FIG. 27]:

177

- BAT_FIRST_PAY_DAY
- BAT_SEC_PAY_DAY
- RESERVE_PERCENTAGE

o If a percentage is entered (greater than zero) into the RESERVE PERCENTAGE field, then there are multiple payments/records to be generated. If RESERVE PERCENTAGE is equal to zero, than there will only be a SINGLE payment performed.

o The ..FIRST.. and ..SEC.. fields, indicate delay in number of days for payments to be generated from the date that the batch itself was PROCESSED.

o The AMOUNT(s) for payment are generated as follows for the FIRST payment, with the SECOND payment record holding the remaining required balance due (if any) from the first payment:

- FIRST PAYMENT AMOUNT = (Total amount to pay) − (Total Amount to Pay)*(RESERVE_PERCENTAGE)

Note: Reserve Percentage multiplier assumes multiplication of PERCENTAGE, regardless of storage numeric format. At the time MoveMoney^{TM} Admin indicates payment to be made, the amounts are taken as complete paid amounts and transactions generated as required, to follow through later as part of the current "MoveMoney^{TM} Admin" Batch. Amounts are paid as complete amounts, and partial amount payments against scheduled payments are not performed by the system. Payments are recorded in the MMC_PAYMENT_LOG table [Ref: FIG. 26; FIG. 27], and status indicator changed in the applicable MC_BATCH_PAY_DUE table [Ref: FIG. 73] record to indicate "Paid". When ALL amounts owed against a patch have been "Paid" in full (all owed amounts against a batch are "zero", then the following indicator can also be changed:

- Table: MMC_BATCH: Field: BAT_CLOSED: "Y"

Once a Batch has been "Closed", it will NOT be "re-opened".

178

In addition to the basic Batch Payment Mechanism, special consideration is given to any amounts incurred against the Seller via Returns that have occurred. In the event that One or more payments have been made against a batch to the SELLER, and the AMOUNT of returns received SUBSEQUENT to payment exceeds the available remaining outstanding amount owed to the Seller, that batch is considered to have gone "NEGATIVE". At this time, funds are drawn off of the applicable Batch's Product Class Reserve to balance the negative amounts (reimbursement to MoveMoney™). If, however, the Product Class Reserves are INSUFFICENT to cover the negative amount, the next available funds are from the RESERVE AMOUNTS of other Product Classes for the SAME Seller. If, in the event, the TOTAL AMOUNT of Reserves for a particular Seller drops to a zero balance (Reserve Amounts can NOT go to a negative balance), then the last alternative is to draw amounts owed from CURRENT outstanding Batches. WHEN THIS OCCURS, the NEXT Scheduled payment against an OPEN Scheduled Batch against the SELLER, the negative balance amount is deducted, and amount added to the back charges in the individual Batch master record.

If the amount owed to the seller against the selected scheduled payment is STILL insufficient to cover the outstanding negative amount, then the process is repeated for EACH scheduled payment for the seller in order of NEXT Scheduled date. For all Scheduled Payments where amounts owed are fully depleted by negative transaction amounts, the BATCH PAYMENT is considered CLOSED, and MMC_PAYMENT_LOG [Ref: FIG. 26; FIG. 27] fields will reflect this information. IF THERE IS INSUFFICIENT FUNDS TO COVER NEGATIVE AMOUNTS AT THIS TIME, THE SELLER THEMSELF IS "NEGATIVE". The STATUS field in the MMC_SELLER_MAS [Ref: FIG. 26; FIG. 27] table will be changed to reflect this. NO PAYMENTS TO SELLERS WILL BE MADE WHEN A SELLER IS INDICATED TO BE NEGATIVE. When a Seller status is negative, all funds specified to be directed to their "holding account" are to be deducted in order to make up the remaining balance owed.

179

There is also an alternative methodology that may be employed here, and the Smarte System™ is designed to handle this methodology as well should it be determined at a later time that in the course of practical application it is preferred. The Product Class Reserve Percentage is utilized in this fashion to not only provide a Risk Management feature against the Returns and amounts owed to the Seller, but applies as well to the Commissions paid out against the accounts as well. In this manner, even if there is NO reserve amount to be applied against a particular Seller's Product Class, this indicator would still function in the manner specified.

This system and method and many of its intended advantages, will be understood from the disclosure herein and it will be apparent that, although the invention and its advantages have been described in detail, various changes, substitutions, and alterations may be made in the form, construction, and/or arrangement of the elements without departing from the spirit and scope of the invention, or sacrificing its material advantages, the form described previously and subsequently herein as being merely a preferred or exemplary embodiment thereof.

180